UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO CONSTITUCIONAL

O DIREITO FUNDAMENTAL À PRIVACIDADE ANTE A MONETIZAÇÃO DE DADOS PESSOAIS NA INTERNET: APONTAMENTOS LEGAIS PARA UMA PERSPECTIVA REGULATÓRIA

Mestrando: Victor M. Barros de Carvalho
Orientador: Prof. Dr. Ivan Lira de Carvalho

UFRN
Natal, 2018

VICTOR MIGUEL BARROS DE CARVALHO

O DIREITO FUNDAMENTAL À PRIVACIDADE ANTE A MONETIZAÇÃO DE DADOS PESSOAIS NA INTERNET: APONTAMENTOS LEGAIS PARA UMA PERSPECTIVA REGULATÓRIA

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre em Direito pelo Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Norte – UFRN.

Orientador: Prof. Dr. Ivan Lira de Carvalho

UFRN
Natal, 2018

Universidade Federal do Rio Grande do Norte - UFRN
Sistema de Bibliotecas - SISBI
Catalogação de Publicação na Fonte. UFRN - Biblioteca Setorial do Centro Ciências Sociais Aplicadas - CCSA

Carvalho, Victor Miguel Barros de.

O Direito fundamental à privacidade ante a monetização de dados pessoais na internet: apontamentos legais para uma perspectiva regulatória / Victor Miguel Barros de Carvalho. - 2018.

145f.: il.

Dissertação (Mestrado em Direito) - Universidade Federal do Rio Grande do Norte, Centro de Ciências Sociais Aplicadas, Programa de Pós-Graduação em Direito. Natal, RN, 2018.

Orientador: Prof. Dr. Ivan Lira de Carvalho.

1. Direito fundamental - Dissertação. 2. Proteção - Dados pessoais - Dissertação. 3. Monetização - Dissertação. 4. Privacidade - Dissertação. 5. Regulação - Dissertação. I. Carvalho, Ivan Lira de. II. Universidade Federal do Rio Grande do Norte. III. Título.

RN/UF/Biblioteca do CCSA CDU 342.7

Elaborado por Eliane Leal Duarte - CRB-15/355

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
CURSO DE MESTRADO

Mestrando: VICTOR MIGUEL BARROS DE CARVALHO

Título: "O DIREITO FUNDAMENTAL À PRIVACIDADE ANTE A MONETIZAÇÃO DE DADOS PESSOAIS NA INTERNET: APONTAMENTOS LEGAIS PARA UMA PERSPECTIVA REGULATÓRIA"

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Norte, como requisito para a obtenção do título de Mestre em Direito.

Aprovado em: 31/08/18

BANCA EXAMINADORA

Prof. Doutor IVAN LIRA DE CARVALHO – UFRN
Presidente

Prof. Doutor MARCELO ALVES DIAS DE SOUZA – MPF
1º Examinador

Profª. Doutora PATRÍCIA BORBA VILAR GUIMARÃES – UFRN
2º Examinadora

Natal (RN)
Agosto/2018

DEDICATÓRIA

Dedico este trabalho a todos que, matando um dragão por dia, encarando jornadas exaustivas de trabalho, de afazeres domésticos, de cuidado aos filhos, batalham em busca da melhora de suas vidas, da paz dos seus e do desenvolvimento da sociedade; e que, de alguma forma, fazem a Ciência (não somente a Jurídica) deste País.

AGRADECIMENTOS

Os agradecimentos iniciais são devidos a Ele que, em sua infindável bondade e compaixão, tantas bênçãos tem derramado sobre este filho teimoso, cabeça-dura e, algumas vezes, malcriado. Obrigado, Deus, por me conceder a dádiva da vida, do trabalho e das atividades!

Agradeço à minha esposa, Ana Paula de Oliveira Rocha Carvalho: sabes que não existem palavras suficientes, ou que alcancem a intensidade necessária, para dizer o quanto seu apoio foi e continua sendo fundamental; seu amor, sua compreensão, sua aguda inteligência e crítico conhecimento jurídico são inestimáveis. Que essa modesta vitória seja uma das muitas conquistas que lograremos ainda!

Agradeço a Maria da Luz, mãe de coração e sogra querida, por todo carinho e cuidado. Agradecimentos devidos também aos amigos que, de uma forma ou de outra, colaboraram para o sucesso desta empreitada, os quais agradeço na figura do nobre camarada Alan Michel Bezerra Furtunato, sempre solícito, sempre companheiro – e um cheiro para "Tia" Ana! Obrigado especial aos colegas da turma de 2016 do Mestrado em Direito da UFRN, da qual espero ter formado muitas e valiosas amizades, os quais cumprimento nas pessoas dos amigos Ana Luíza Félix, Carlos André, Evilásio Galdino e Leonardo Júnior.

Devo mencionar, sem dúvidas, os Magistrados Natália Torres e Rafael Barros pelas oportunidades preciosas de crescimento, tanto pessoal como profissional: meu enternecido obrigado! Agradecimentos devidos ainda à Magistrada Marina Melo, pela oportunidade e pelo reconhecimento, e à Magistrada Larissa Almeida, igualmente pela oportunidade, confiança, paciência, compreensão e pela chance de aprender pelo exemplo com uma profissional competente, humilde e de tão raro caráter, em nome de quem agradeço aos servidores e funcionários (e estagiários!) da 1ª Vara da Comarca de Santa Cruz/RN.

Agradeço ao professor Dr. Ivan Lira de Carvalho, pelo exemplo de intelectualidade emanado de sua postura – seja na Magistratura, seja na Academia –, e pela coragem de orientar-me neste instigante e complicado desafio. Agradecimentos também ao prof. Dr. Yanko Xavier e à prof. Dra. Patrícia Borba, pelo encorajamento, desde os tempos da graduação, da iniciação científica e do PRH nº 36, à pesquisa e à busca pelo conhecimento; não hei de esquecer, evidentemente, do prof. Dr. Anderson Lanzillo, orientador do meu trabalho de conclusão da graduação e incentivador acadêmico. Meu muito obrigado também ao prof. Dr. Danilo Doneda, pela cordial atenção e por tão gentilmente disponibilizar sua

paradigmática – e já esgotada – obra seminal para o estudo da privacidade e dos dados pessoais.

Por fim, agradecimentos sem tamanho aos heróis e heroínas anônimos(as) que fazem o Sci-Hub e a Library Genesis: posso afirmar que, sem o abnegado esforço de vocês pela democratização da Ciência, este trabalho não seria o mesmo!

Obrigado!

"Furthermore, as I have already said, no secret will ever be as safe when its protection is a matter of human integrity, as when it was dependent on the difficulties of scientific discovery itself".
Norbert Wiener, The Human Use of Human Beings

RESUMO

O presente trabalho tem por objeto lançar uma visão jurídica sobre o cenário de monetização de dados pessoais, com vistas a sugerir perspectivas regulatórias para estas atividades econômicas e almejando, com isto, conferir maior proteção ao direito fundamental à privacidade. Parte da atual problemática do uso econômico dos dados pessoais e a preocupação com o direito fundamental à privacidade, que encontra-se em risco de violação ante as diversas práticas de tratamento destes dados – risco este maximizado e potencializado, principalmente, com a democratização das redes sociais virtuais. Tem por objetivo principal sugerir, em termos gerais, perspectivas para a regulação da utilização com fins econômicos de dados pessoais. Dentre seus objetivos específicos estão: elaborar breve evolução do direito fundamental à privacidade até a proteção dos dados pessoais; abordar a conjuntura relativa ao tratamento de dados, amparada nos paradigmas da sociedade em rede, sociedade informacional, ciberespaço, convergência digital, dataísmo e conceitos correlatos; demonstrar através de alguns exemplos como se dá a utilização de dados pessoais em modelos de negócio e como surge a preocupação com sua proteção e salvaguarda da privacidade; realizar um apanhado dos diplomas legais atinentes à temática no Brasil, analisando-os sob a ótica da monetização e proteção dos dados pessoais; extrair do corpo legal disponível capacidades regulatórias para o cenário brasileiro de monetização de dados pessoais, tendo em vista não só a proteção da privacidade, mas também dos valores a ela conexos. Como metodologia, baseia-se em uma leitura crítica do material teórico levantado: dos diplomas legais nacionais que têm atinência com a temática, da doutrina mais abalizada em termos de privacidade, dados pessoais, sociedade informacional e regulação, e de notícias de portais especializados, utilizados unicamente para ilustrar situações demasiadamente contemporâneas e que a Ciência Jurídica ainda não foi capaz de alcançar. Utiliza como pressuposto crítico de análise o imperativo de proteção do direito fundamental à privacidade neste cenário de monetização de dados pessoais. Neste intuito, insere este direito nos paradigmas da sociedade da informação, sociedade em rede e ciberespaço para, contextualizando-o, dele extrair um conteúdo protetivo capaz de abarcar as complexidades próprias deste cenário de protagonismo dos dados e informações. Após, e a partir da análise do arcabouço legal nacional e considerando as construções teóricas previamente realizadas, que sugerem um cenário de extremo risco ao direito fundamental à privacidade e às liberdades que este pressupõe (liberdade de pensamento, liberdade política, religiosa, sexual, entre outras) por meio de práticas como a *surveillance*, já chamada até mesmo de *dataveillance*, busca propor apontamentos regulatórios aptos a abordar o tratamento de dados pessoais, capazes de proteger a privacidade dos titulares dos dados. Indica certas proposituras, gerais, abstratas e atemporais, para orientar a atuação do Estado neste intento: por exemplo, a necessária e forte presença Estatal na regulação destes serviços, a valorização de princípios como o da autodeterminação informativa e do livre consentimento, e uma regulação cada vez mais baseada no postulado da *privacy by design*. Concluiu, apesar da edição da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), pela necessidade de criação de uma Autoridade Nacional de Proteção de Dados para centralizar, organizar e conferir maior força ao *enforcement* da legislação nacional, assim como sugerindo uma atuação regulatória pautada na perspectiva do risco e do "*code is law*", de Lawrence Lessig.

Palavras-chave: Dados pessoais; monetização; proteção; privacidade; regulação.

ABSTRACT

The object of this dissertation is to cast a legal view over the personal data monetization scenario, intending to suggest regulatory perspectives to such economic activities and aiming to contribute to the protection of the right to privacy. Its starting point is the resulting problematic of this scenario and the concern over privacy protection, which is in grave risk of violation because of the numerous data practices – a risk that is potentialized, mainly, on account of the democratization of virtual social networks. Its main objective is to suggest, in broad terms, regulatory perspectives over economic uses of personal data. Among its specific objectives: elaborate a brief overview on the evolution of the fundamental right to privacy, from its origins to the data protection concerns; approach the data treatment conjuncture, based on the networked society, informational society, cyberspace, digital convergence, dataism and other correlated paradigms; demonstrate through a few examples how personal data monetization occurs in some business models and why the privacy concern arises; make a collection of the laws, bills and normatives that relate to the object, analyzing them under the perspective of personal data monetization and protection; extract from the available legal body regulatory possibilities to the Brazilian personal data monetization scenario, aiming not only to contribute on the protection of privacy, but also its attached values. As a work methodology, it utilizes a critical review of the collected theoretic material: of the legal normatives; the state-of-the-art works and authors in terms of privacy, personal data, informational society and regulation; and of specialized portals news, used as a mean to illustrate certain contemporary situations that the Legal Science is yet to grasp. The work utilizes as a critical premisse in its analysis the imperative of privacy protection in this scenario of data protection. With this intent, the work inserts the right to privacy in the informational society, network society and cyberspace paradigms, contextualizing it, in order to extract from this contextualization a protective content of this right, able to comprehend the inherent complexities of this personal data monetization scenario. After that, considering the previous legal analysis and theoretic constructions, that suggests a scenario of extreme risk to the fundamental right to privacy and the liberties it encompasses (freedom of thought, political freedom, religious, sexual, among others) through practices such as surveillance, that is even called dataveillance by some, aims to propose regulatory guidances fit to approach the data monetization scenario, able to protect the privacy of the data subjects. The work indicates certain general, broad and perennial propositures, aiming to orient the State procedures: as an example, the need of a strong State presence in these services regulation, the praise of principles such as the informational self-determination and free consent, and a regulatory performance more based on the concept of privacy by design. It concludes, in spite of the Brazilian General Data Protection Regulation publishing, stressing the need to create a Data Protection National Authority, capable of centralizing, organizing and empowering the enforcement of the national legislation, as well as suggesting a regulatory proceeding more based on the risk perspective and the Lawrence Lessig's "code is law" perspective.

Key-words: Monetization; personal data; privacy; protection; regulation.

LISTA DE ABREVIATURAS

ANATEL – Agência Nacional de Telecomunicações

ANPD – Autoridade Nacional de Proteção de Dados

CGI.br – Comitê Gestor da Internet no Brasil

CNJ – Conselho Nacional de Justiça

CNMP – Conselho Nacional do Ministério Público

CNPD – Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GDPR – General Data Protection Regulation (Lei Geral de Proteção de Dados da União Europeia)

IoT – Internet of Things (Internet das Coisas)

LGPD – Lei Geral de Proteção de Dados

MCI – Marco Civil da Internet

SENACON – Secretaria Nacional do Consumidor

SBDC – Sistema Brasileiro de Defesa da Concorrência

TIC – Tecnologias da Informação e Comunicação

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

É inegável a mudança de paradigmas que a sociedade vivencia nos primeiros anos do século XXI – principalmente após o advento, democratização e difusão da internet. Diferentes ramos do conhecimento cunharam termos distintos para tentar conceituar este cenário de cada vez maior preponderância da internet e das Tecnologias da Informação e Comunicação nos inúmeros setores da sociedade: Manuel Castells chamou-o de sociedade da informação (ou sociedade em rede); Pierre Lévy, de cibercultura e ciberespaço – este último conceito também utilizado por Daniel J. Solove, Lawrence Lessig e originalmente batizado por John Perry Barlow; Andrew Murray, de convergência digital; Yuval Noah Harari, de dataísmo; isto apenas para citar alguns dos cientistas que se debruçaram sobre o tema.

Mas independente da nomenclatura e das peculiaridades inerentes a cada análise, tais definições encontram um denominador comum precisamente no protagonismo das ferramentas de TIC, principalmente a internet, e dos dados e informações gerados e utilizados em tal panorama.

Este protagonismo vem transformando o modo como vários âmbitos da sociedade se manifestam e tocam seus processos: a cultura, os relacionamentos, o comportamento, e até mesmo a política e a economia vem experimentando intensas influências e modificações. As relações se dão, gradativamente, mais no âmbito digital (ou, utilizando um termo mais apropriado, no ciberespaço), gerando com isto uma quantidade abissal de dados e informações.

Daí se falar, por exemplo, em *Internet of Things* (internet das coisas) para representar o alcance da interconectividade entre dispositivos, e em *Big Data*, para tratar do cenário de vastas quantidades de dados e informações, assim como das soluções tecnológicas para o seu aproveitamento: termos como algoritmos, *machine learning* (aprendizado automático, aprendizado de máquina) e *business inteligence* (tomar decisões de negócios com base em análise de dados) estão em crescente voga. O dado passou a ser útil, a ter valor; sua análise e tratamento também passam a ser preciosos. Neste cenário, então, têm-se considerado os dados produzidos como uma matéria-prima. Certos empreendedores foram além, apontando-os como sendo o "novo petróleo".

Em tal quadro de produção de dados, o cidadão nele inserido se vê compelido não só a consumir informações e dados, mas também a produzi-los, entregá-los e fornecê-los. Somos exigidos, por exemplo, pelas redes sociais virtuais (como o *Facebook, Twitter, Instagram*, entre outras) a entregar inúmeros dados pessoais em contrapartida pelo acesso e uso. Inúmeros outros serviços oferecidos na internet (como guias GPS, buscadores, plataformas de mensagens e de comércio eletrônico, etc) também exigem que forneçamos dados – e que continuemos a produzi-los.

Isto não é a toa: como se adiantou, os dados, tidos como matéria-prima, são de importância fulcral para tais companhias, que os monetizam de diferentes maneiras. A mais conhecida e difundida destas maneiras é a publicidade dirigida, que, em brevíssimo resumo, é a prática da análise dos dados e informações pessoais de indivíduos ou grupos para oferecer a publicidade mais relevante possível em relação a suas preferências.

Assim, por um lado, os dados acabam servindo como moeda de troca para os internautas que usufruem gratuitamente de serviços; por outro, a entrega deliberada (e por vezes excessivamente ingênua e voluntária) dos dados pessoais suscita certa preocupação com a privacidade dos usuários destes serviços – preocupação que não é infundada, principalmente quando se considera os casos de espionagem e exploração dos dados pessoais tornados públicos pelo *WikiLeaks* e pelo *whistleblower* (denunciante) americano Edward Snowden, não olvidando-se também do escândalo envolvendo a *Cambridge Analytica* e o *Facebook*. Este último *case*, por sua magnitude, teve o mérito de atrair maior atenção pública para a necessidade de proteção dos dados pessoais, tendo o CEO do *Facebook*, Mark Zuckerberg, sido inclusive intimado a depôr no Congresso norte-americano.

Nestes paradigmáticos casos, verificou-se que agências de inteligência de diversos governos mundiais estavam coletando e analisando os dados pessoais de cidadãos (e até mesmo de mandatários de outras nações) com finalidades de vigilância. As justificativas, ventiladas após as denúncias, rodeavam o lugar comum do combate ao terrorismo e proteção da segurança nacional. A Cambridge Analytica, por sua vez, foi acusada de utilizar dados pessoais de milhões de usuários do Facebook para influenciar a saída do Reino Unido da União Europeia (caso cunhado de *Brexit*) e de manipular os eleitores dos Estados Unidos da América para elegerem o então candidato Donald Trump presidente daquela nação. São casos que denotam o perigo que a prática do uso de dados pessoais ostenta para a democracia e seus rumos.

Outro receio, mais próximo do cidadão médio, pode ser retirado do uso dos dados médicos, hospitalares e dados de qualquer maneira relacionados à saúde: imaginando-se, por exemplo, que uma seguradora de saúde pode coletar, utilizar, reunir e conjugar dados de registros das consultas médicas, de resultados de exames laboratoriais, das compras realizadas em farmácias (rastreadas através do CPF e números de cartões de crédito), de pesquisas em sites de busca e até mesmo de hábitos possivelmente danosos à saúde expostos nas redes sociais, é possível conjecturar que, a depender dos resultados obtidos com tais dados, a seguradora poderia estipular o valor da apólice ofertada de acordo com os parâmetros alcançados.

A privacidade do cidadão, possivelmente exposta na internet através dos dados pessoais e potencialmente devassada por meio de tal prática exemplificada, poderia infligir-lhe severos

prejuízos. O titular dos dados não padeceria somente em termos de exclusão em serviços de seguro, mas também na busca de emprego e na socialização.

Ante este cenário de utilização com objetivos monetários (assim como outros, potencialmente mais obscuros e escusos) dos dados pessoais e a preocupação com a salvaguarda do direito fundamental à privacidade que decorre da proteção de tais dados, cabe à ciência jurídica despender esforços na busca por soluções que acomodem os diferentes atores, as diferentes searas e os diferentes direitos que concorrem em tal panorama. E uma das principais perspectivas de atuação jurídica, mormente quando se abordam temas com conotações econômicas, se traduz na regulação, justificada pelo ferramental institucional e legal de que dispõe para a defesa de direitos fundamentais e de interesses coletivos e difusos.

Este é – ressalvadas as dificuldades inerentes a uma análise de tema tão amplo, complexo, profuso e plural, e considerada a velocidade das mudanças e avanços próprios da sociedade em rede – o objeto da presente dissertação: se debruçar sobre esta multidisciplinar temática e, sob um viés jurídico, inquirir e procurar delinear, ou ao menos esboçar, perspectivas e nortes regulatórios para o uso econômico dos dados pessoais no Brasil.

Como objetivo principal, o trabalho esquadrinha o atual cenário de monetização de dados pessoais no Brasil do ponto de vista jurídico, a partir das leis e normativas atinentes, bem como marcos, entes e institutos regulamentadores disponíveis, com o fito de sugerir, em termos gerais, perspectivas para a regulação da utilização com fins econômicos de dados pessoais, sobretudo considerada a necessidade de proteção do direito fundamental à privacidade.

Entre seus objetivos específicos, a presente pesquisa tece ligeiros comentários sobre a evolução do direito fundamental à privacidade até a proteção dos dados pessoais; aborda a conjuntura relativa ao tratamento de dados, amparada nos paradigmas da sociedade em rede, sociedade informacional, ciberespaço, convergência digital, dataísmo e conceitos correlatos, demonstrando através de alguns exemplos como se dá a utilização de dados pessoais em modelos de negócio e como surge a preocupação com sua proteção e salvaguarda da privacidade; realiza um apanhado dos diplomas legais atinentes à temática no Brasil, analisando-os sob a ótica da monetização e proteção dos dados pessoais; extrai do corpo legal disponível capacidades regulatórias para o cenário brasileiro de monetização de dados pessoais, tendo em vista não só a proteção da privacidade, mas também dos seus valores conexos; e sugere, ante a construção teórica supra, elementos orientadores para uma regulação que viabilize a proteção do direito fundamental à privacidade no quadro sob análise, apontando nortes genéricos, abstratos e atemporais que se adéquem ao panorama brasileiro.

Para tanto, faz uma revisão bibliográfica da literatura científica concernente aos temas ora abordados, com a coleta e análise dos diplomas legais nacionais atinentes, valendo-se também, pela necessidade oriunda da contemporaneidade e volatilidade do tema, de notícias publicadas em portais especializados, almejando com elas unicamente ilustrar certas questões suscitadas no cenário estudado, sobretudo por inexistir suficiente esforço acadêmico acerca de casos tão recentes. Necessário ressaltar que a utilização de notícias de portais especializados funciona unicamente para ilustrar quadros fáticos, nelas não apoiando o trabalho as suas construções teóricas.

A metodologia utilizada para alcançar os objetivos propostos baseia-se em uma abordagem crítico-descritiva das leituras, tomando por pressuposto crítico a preponderância e necessidade de proteção dos direitos fundamentais, sobretudo da privacidade, sobre as demais situações do cenário estudado. Após estas leituras, construiu-se a linha teórica defendida com base em argumentos de autoridade extraídos das produções científicas consultadas, auxiliada também por uma interpretação dos diplomas legais através dos processos lógico e sistemático. Utiliza ainda, como ferramental apto a abordar as abstratas e complexas situações estudadas, metáforas e analogias para descrever tanto hipóteses aferidas como sugestões e soluções alcançadas.

Desta forma, o capítulo de número dois aborda, por lei e doutrina, o direito fundamental à privacidade e o desenvolvimento, no ordenamento jurídico pátrio, da sua proteção e dos dados pessoais.

O capítulo de número três procura expor o panorama no qual encontra-se inserido este direito fundamental e a preocupação com sua tutela, esboçando, ainda, o cenário de monetização de dados de maneira a situar pragmaticamente o trabalho. O capítulo de número quatro traz o resultado da pesquisa acerca de elementos e nortes regulatórios, bem como sua relação com a monetização dos dados pessoais e sugere, ao final, perspectivas amplas e gerais de regulação para tal cenário no país, visando sobretudo posicionar o trabalho em um patamar de atemporalidade e utilidade, precavendo-se ante a altamente veloz taxa de atualização e modificação do tema estudado e às críticas de inaptidão do Estado e suas capacidades para lidar com situações disruptivas.

O trabalho conclui no sentido de que, ante a complexidade do cenário de monetização de dados pessoais e a premência de se resguardar o direito fundamental à privacidade e seus valores conexos, é necessária uma atuação estatal de maior proeminência. Entende que, no paradigma da sociedade informacional, pautada cada vez mais no protagonismo dos dados e das informações, exsurge a necessidade de proteção dos dados pessoais como elemento corolário do direito à privacidade, em razão da capacidade que o tratamento destes tem para descortinar aspectos íntimos e privados dos titulares, pondo em risco, igualmente, valores inerentes à privacidade – notadamente a liberdade e as prerrogativas que esta encerra.

Esboça uma metáfora em termos de luz e sombra para explicitar como o conteúdo protetivo da privacidade, a sombra, projetada pelos diplomas e institutos legais que a tutelam, possui a liberdade de amoldar-se de acordo com as situações específicas, apontando, destarte, a necessidade de contextualização para preenchimento do conteúdo protetivo deste direito; a luz, neste caso, representa as potenciais violações do direito à privacidade. Pondera que esta concepção de privacidade seria adequada para atender às situações advindas da monetização de dados pessoais.

Neste intento, aborda o paradigma no qual encontra-se inserida a monetização de dados pessoais de forma que ficassem explícitas algumas características básicas, como o protagonismo das Tecnologias da Informação e da Comunicação, da internet, dos dados e das informações e do valor que estes ostentam, a intensa interconectividade, a intensa dinâmica de fluxo das redes, o caráter supranacional das redes e as dificuldades que tal situação traz para a normatização e regulação deste cenário.

Por fim, defende, a partir da constatação do valor atribuído aos dados pessoais e dos perigos que a sua monetização ostenta, que os dados não são o novo petróleo mas, sim, o novo urânio, em razão dos perigos potenciais à privacidade e a seus valores conexos, como o livre desenvolvimento da personalidade, a liberdade de pensamento, liberdade de crença, liberdade sexual, liberdade política, entre outros. Partindo igualmente desta constatação é que argumenta pela necessidade de regulação das atividades monetizadoras de dados pessoais, com a finalidade de proteger a privacidade e seus valores conexos, valendo-se para tanto de postulados abstratos e atemporais.

2 O DIREITO FUNDAMENTAL À PRIVACIDADE E A PROTEÇÃO AOS DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

Em sua obra "Recordações da Casa dos Mortos", Fiódor Dostoiévski reconta parte do período em que ficou preso em um campo de prisioneiros da Sibéria. A certo momento, faz mostrar ao leitor sua intensa infelicidade com aquela situação, apontando um aspecto que particularmente o incomodava: dizia ele que não havia tormento maior do que não conseguir ficar sozinho um momento sequer – seja na presença de companheiros de cárcere ou sob a vigia dos guardas, a impossibilidade de um momento de privacidade e quietude o atormentava[1].

É de se imaginar o que diria Dostoiévski frente a influência das Tecnologias da Informação e Comunicação na sociedade, que impulsiona o uso da internet em inúmeros dispositivos, apetrechos e instrumentos e torna a presença pessoal[2] sentida mesmo quando fisicamente distante: talvez, teria dito que vivemos um frenesi exibicionista, fazendo expandir aquele incômodo do cárcere para a vida cotidiana, sem nunca ficarmos efetivamente sós, sem nunca possuir um momento sem se revelar – há sempre uma mensagem a mandar, um trecho de áudio, uma foto ou vídeo, uma "curtida", um "seguir", uma novidade, uma notificação; sempre um meio para se fazer presente e para ser encontrado.

Ao literato russo, que estimava a solidão e os momentos de meditação introvertida, seria talvez impensável conceber a rotina de quase metade[3] da população brasileira – impressionantes 100 milhões de pessoas – que estão acessando a internet e nela interagindo, participando de redes sociais virtuais e potencialmente expondo, produzindo e reproduzindo, em aproximadas (e

---

[1] "Eu jamais poderia, por exemplo, imaginar tormento maior do que não poder ficar sozinho um momento, ao menos, nos dez anos da minha sentença. No trabalho, vigiado; no presídio, com a companhia dos outros duzentos condenados; e nunca, nem uma só vez, a solidão! Contudo, tive de me acostumar.". DOSTOIÉVSKI, Fiódor. **Recordações da Casa dos Mortos**. Trad.: Nicolau S. Peticov. São Paulo: Nova Alexandria, 2005. Não paginado (epub).

[2] "Se alimenta lo «público» para dar sentido a lo «privado». Se exhibe un conjunto de informaciones personales, el cuerpo electrónico, como se exhibe el cuerpo físico mediante los tatuajes, los piercings y outras señas de identidad. La identidad se hace comunicación". RODOTÀ, Stefano. **El derecho a tener derechos**. Tradução de José Manuel Revuelta Lopez. 1. ed. Madrid: Trotta, 2014. p. 296

[3] "Praticamente a metade dos brasileiros, 48%, usa internet. O percentual de pessoas que a utilizam todos dos dias cresceu de 26% na PBM 2014 para 37% na PBM 2015". BRASIL. Presidência da República. Secretaria de Comunicação Social. **Pesquisa brasileira de mídia 2015**: hábitos de consumo de mídia pela população brasileira. Brasília: Secom, 2014. p. 7

impressionantes) vinte e oito horas por semana[4], inúmeros dados, dentre os quais os dados pessoais[5].

Essa vivência no ciberespaço[6] fez surgir uma nova preocupação quanto à privacidade dos usuários da internet e de seus serviços, forçando o desenvolvimento do Direito[7] neste aspecto e modificando os paradigmas para a tutela da privacidade – e até mesmo o seu conceito[8].

Ademais, a pesquisa com estes complexos paradigmas surge, não raras vezes, um pouco confusa em termos de separação dos temas: falar em privacidade é tratar, direta ou indiretamente, de relações sociais, de fluxos econômicos, do funcionamento de constructos burocráticos (sejam eles governamentais ou privados) e de instrumentos legais e regulatórios.

Estudar a privacidade perpassa ainda pela intrincada trama das relações de mercado e de políticas internacionais, com as suas variantes de influência e normatização. A globalização, após o advento da internet, reagiu como um atleta que toma esteroides anabolizantes: seus efeitos foram enormemente potencializados, sendo disto prova, por exemplo, a recente implementação da GDPR (*General Data Protection Regulation* – Lei Geral de Proteção de Dados, em tradução livre) da União Europeia como forma de adequar-se ao cenário em comento.

Os termos, condições e imposições legais exaradas pela União Europeia tiveram efeitos que repercutiram no mundo inteiro, desconsiderando, por vezes, as normas e regulações de outras nações. Após a implementação deste diploma regulador no âmbito de alguns países europeus, várias empresas e instituições de outros países – mas que lidam com dados de cidadãos europeus (visto que a internet tende a ignorar as barreiras geográficas e limítrofes das divisas nacionais) – tiveram de adequar suas práticas às novas determinações legais, ao passo que outras, seja por incapacidade financeira, técnica, legal ou por vontade de economizar frente ao esforço de *compliance* (conformidade, em tradução livre), simplesmente passaram a bloquear e negar acesso aos

---

[4] "Os usuários das novas mídias ficam conectados, em média, 4h59 por dia durante a semana e 4h24 nos finais de semana". Ibidem, p. 7

[5] Segundo Marcel Leonardi, "dado pessoal é o dado relacionado a um indivíduo identificado ou identificável, independentemente do suporte em que se encontre registrado (escrita, imagem, som ou vídeo). Entende-se por identificado o indivíduo que já é conhecido, e por identificável a pessoa que pode ser conhecida diretamente pelo próprio possuidor de seus dados, ou indiretamente através de recursos e meios à disposição de terceiros". LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2011. p. 76

[6] Pierre Lévy explica o conceito como sendo um novo meio de comunicação permitido pela interconexão de computadores em escala planetária. Este e outros conceitos serão abordados em maior detalhe em capítulo posterior. Cf.: LÉVY, Pierre. **Cibercultura**. Trad. Carlos Irineu da Costa. São Paulo: 34, 1999. p. 17

[7] "Os avanços tecnológicos também tornam obsoletos certos dilemas jurídicos, ao mesmo tempo em que criam inúmeros outros." LEONARDI, op. cit., p. 27

[8] "doutrina e a jurisprudência vêm paulatinamente reconhecendo que a privacidade relaciona-se com uma série de interesses distintos, o que modifica substancialmente seu perfil tradicional". Ibidem, p. 79

internautas com acesso originário da Europa[9]. Tal situação ressalta sobremaneira o nível de complexidade deste tema.

Assim, de forma a não usurpar o conteúdo do capítulo seguinte e atendo-se à metodologia proposta, passa-se a analisar, no momento que segue, certos aspectos históricos e conceituais que envolvem o direito fundamental à privacidade, os valores a ele conexos, os diplomas legais normatizantes no Brasil e a discussão que levou até a necessidade de proteção dos dados pessoais como corolário da proteção à privacidade[10].

2.1 ASPECTOS HISTÓRICOS E CONCEITUAIS DO DIREITO FUNDAMENTAL À PRIVACIDADE

Falar em privacidade como direito não é tarefa simples. Trata-se de um direito com conteúdo de tutela amplo, mutável, e que abrange uma vasta gama de situações[11]; que envolve

[9] HERN, Alex; WATERSON, Jim. **Sites block users, shut down activities and flood inboxes as GDPR rules loom**. Disponível em: <https://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect>. Acesso em: 07 jun. 2018.
SANDERS, James. **To save thousands on GDPR compliance, some companies are blocking all EU users**. Disponível em: <https://www.techrepublic.com/article/to-save-thousands-on-gdpr-compliance-some-companies-are-blocking-all-eu-users/>. Acesso em: 07 jun. 2018.
KOTTASOVÁ, Ivana. **These companies are getting killed by GDPR**. Disponível em: <http://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html>. Acesso em: 07 jun. 2018.
TECHDIRT. **Companies Respond To The GDPR By Blocking All EU Users**. Disponível em: <https://abovethelaw.com/2018/05/companies-respond-to-the-gdpr-by-blocking-all-eu-users/>. Acesso em: 07 jun. 2018.

[10] "a necessidade de funcionalização da proteção da privacidade faz, portanto, com que ela originasse uma disciplina da proteção de dados pessoais, que compreende pressupostos ontológicos idênticos aos da própria proteção da privacidade: pode-se dizer que é a sua 'continuação por outros meios'". DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 27

[11] "Assim como outras expressões que refletem conceitos jurídicos indeterminados, tais como liberdade e dignidade da pessoa humana, a palavra privacidade parece englobar tudo, mas aparenta ser nada em si mesma; seu conceito estaria recheado de 'ambiguidades perniciosas'". LEONARDI, op. cit., p. 47

várias áreas do conhecimento[12]. É uma problemática que parte da própria denominação pela doutrina[13] e pela ausência de conceituação pela legislação[14].

Não obstante, o processo histórico evolutivo delineou as balizas que conformam este direito, contando com períodos-chave para sua consolidação e valendo-se da contribuição doutrinária para sua consecução. Seria de todo ineficiente ao objetivo proposto e tanto quanto injusto com a obra de certos autores despender muitas páginas com uma linha evolucionária deste direito demasiadamente detalhada: isto porque os trabalhos dos professores Danilo Doneda, Laura Schertel Mendes e Marcel Leonardi já o fizeram[15] com tremenda qualidade, de forma que remeter-se a estas obras seminais é indicado a quem deseja se aprofundar nesta temática em minúcias.

Nos interessa, aqui, um apanhado teórico que permita reunir fundamentos da privacidade minimamente adequados ao panorama atual de monetização de dados pessoais[16] e que subsuma-se à efetivação deste direito fundamental em uma perspectiva de regulação.

Neste azo, todavia, é possível adiantar, por um lado, que o esforço conceitual produzido não alcançará (nem a isso se presta o presente trabalho) um conceito ideal e fechado de privacidade, vez que a própria história deste direito demonstra a falibilidade de tal empreendimento; e, de outro – na perspectiva do ciberespaço e da monetização dos dados pessoais – que é permitido pensar em uma dupla frente de proteção a este direito, originada precisamente do cenário que ora se estuda: uma frente destinada à tutela e garantia da privacidade do indivíduo e, a outra, à proteção de grupos e coletividades.

---

[12] "The landscape of theoretical work on privacy is vast, spanning disciplines from philosophy to po liti cal science, politi cal and legal theory, media and information studies, and, increasingly, computer science and engineering". NISSENBAUM, Helen. **Privacy in context:** technology, policy and the integrity of social life. Stanford: Stanford University, 2010. p. 67

[13] "A doutrina brasileira emprega uma profusão de termos distintos para se referir à privacidade. Fala-se em "vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e até mesmo 'privatividade' e 'privaticidade', entre outros. O mesmo ocorre na doutrina estrangeira, que se socorre de uma variedade de expressões para se referir à privacidade. Na Alemanha, tem-se die Privatsphäre, separando a autonomia individual e a vida social; […] em Portugal, diz-se reserva da intimidade da vida privada e privacidade". LEONARDI, op. cit., p. 46.
"Também na doutrina brasileira não há consenso sobre a denominação desse direito, pois a própria Constituição Federal propicia o debate terminológico sobre o direito à privacidade, ao determinar em seu artigo 5º, X, que são invioláveis a vida privada e a intimidade. Nesse sentido, a norma suprema suscita a discussão acerca do sentido de cada uma das expressões: designariam 'vida privada' e 'intimidade' bens jurídicos distintos?". MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. Dissertação (Mestrado em Direito). Brasília: Universidade de Brasília, 2008. p. 19

[14] "A Constituição Federal de 1988 não utiliza a expressão privacidade; declara invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação. Do mesmo modo, o Código Civil de 2002 não menciona em nenhum momento a palavra privacidade; declara que a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma". Ibidem, p. 46.

[15] DONEDA, 2006, op. cit.; LEONARDI, op. cit.; MENDES, op. cit.

[16] Entendemos por monetização de dados pessoais toda a prática com base nos dados pessoais que visa retornos financeiros. Exemplos são a publicidade dirigida, o tratamento e a comercialização de dados pessoais. No capítulo de número três se aborda com maior detalhismo esta temática.

Dito isto, temos que a privacidade como conceito (e, posteriormente, como direito) é um constructo da época moderna, que tem por marco temporal inicial o século XIX[17] e suas profundas transformações: do rural ao urbano, das vilas às cidades, do trabalho campesino ao trabalho fabril; da redução de espaços comunitários em desfavor do espaço privado (na acepção cível da expressão, em contraponto ao público), do Antigo Regime à nova ordem burguesa. É um direito que tem sua gênese com as demandas trazidas pela burguesia[18], gestado na esteira da valorização do indivíduo[19], de seu desenvolvimento, de seu direito à propriedade privada, à proteção contra a interferência estatal, à liberdade e a certo âmbito de autonomia no dirigir de sua própria vida.

Não à toa, um dos primeiros esforços doutrinários pelo reconhecimento da privacidade como direito é o artigo publicado na *Harvard Law Review* por Samuel Warren e Louis Brandeis[20], intitulado "The Right to Privacy" (O Direito à Privacidade), em 1890. No artigo, extremamente difundido e citado pelos estudiosos deste tema, os autores defendem a possibilidade de o indivíduo se resguardar contra a invasão[21] de certas áreas da privacidade e da intimidade então permitida pelo avanço tecnológico da época, traduzido principalmente nas câmeras fotográficas, cada vez mais portáteis, que viabilizavam uma devassa maior do cotidiano de pessoas proeminentes[22].

---

[17] "Privacidade, individualismo, civilização, familiaridade, eis as variáveis de uma história da vida privada concebida como problemática de pesquisa referida à Época Moderna, mas sobretudo à história ocidental do século XVIII em diante. […] Como ponto de partida, o final da Idade Média, tempo em que o indivíduo se enquadrava em solidariedades coletivas, feudais, comunitárias: as solidariedades da comunidade senhorial, as solidariedades entre linhagens, os vínculos dê vassalagem. Solidariedades e vínculos que encerram o indivíduo ou a família num mundo que não é nem público nem privado. O ponto de chegada é o século XIX: a sociedade se transformou numa população anônima onde as pessoas já não mais se conhecem. O trabalho, o lazer e o convívio se tornam atividades separadas em compartimentos estanques. O indivíduo procura proteger-se, então, dos olhares dos outros: escolhe livremente, ou pensa que escolhe, seu estilo de vida, ou se recolhe na família, refúgio do espaço privado". VAINFAS, Ronaldo. **História da vida privada**: dilemas, paradigmas, escalas. Anais do Museu Paulista. São Paulo. n. sér. v. 4 p. 9-27 jan./dez. 1996. p. 17

[18] "É nesse sentido que ela foi considerada por muito tempo como um direito tipicamente burguês, na medida em que sobressaíam as suas características de direito negativo, como a exigência absoluta de abstenção do Estado na esfera privada individual para a sua garantia". MENDES, 2008, op. cit., p. 16

[19] "Não havia realmente lugar para a tutela jurídica da privacidade em sociedades que confiavam sua regulação a outros mecanismos – fossem estes a rigidez da hierarquia social ou então a própria arquitetura dos espaços públicos e privados […] O despertar do direito para a privacidade ocorreu justamente num período em que mudou a percepção da pessoa humana pelo ordenamento, do qual ela passou a ocupar papel central e ao qual se seguiu a juridificação de vários aspectos de seu cotidiano" DONEDA, 2006, *op. cit.*, p. 8

[20] WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. **Harvard Law Review**, v. IV, dez. 1890, n. 5. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 10 jan. 2017.

[21] "O início dos debates doutrinários sobre o direito à privacidade ocorreu como conseqüência da utilização de novas técnicas e instrumentos tecnológicos, que passaram a possibilitar o acesso e a divulgação de fatos relativos à esfera privada do indivíduo de uma forma anteriormente impensável. Isso pode ser percebido com o pioneiro artigo sobre privacidade de Warren e Brandeis, publicado na Harvard Law Review e intitulado "The Right to Privacy", no qual os autores denunciavam como a fotografia, os jornais e aparatos tecnológicos tinham invadido os sagrados domínios da vida privada e doméstica". MENDES, 2008, *op. cit.*, p. 14

[22] "Há muito debate em torno da motivação de Warren e Brandies para a publicação do artigo dedicado ao privacy. Alguns estudiosos especulam que foi uma resposta ao aumento de sensacionalismo da imprensa em geral. Outros apontam que seria uma reação direta aos abusos cometidos pela imprensa contra a família de Warren, uma das mais influentes na sociedade de Boston do final do século XIX". ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do right of privacy nos estados unidos. **Revista Brasileira de Direito Civil** | ISSN 2358-6974 |

Este trabalho foi um dos precursores do "*right to be let alone*", ou "direito à ser deixado só", que estipula a privacidade como sendo a capacidade de o indivíduo ser deixado em paz, de exercer sua solitude e viver de acordo com seus desejos[23], filtrando as influências com as quais deseja ter ou manter contato.

Posteriormente, no pós-segunda grande guerra mundial, a privacidade é positivada em diversos tratados e acordos internacionais, devendo-se dentre eles destacar a Declaração Universal dos Direitos do Homem, de 1948, que previu em seu art. XII a proteção dos indivíduos contra "ingerências arbitrárias em sua vida privada"[24].

Com o passar do tempo e com o desenvolver das tecnologias e das interações humanas, novas questões surgiram em relação ao direito à privacidade, demandando novas respostas e soluções na tutela deste aspecto da personalidade do indivíduo[25], tornando, se não obsoletas, talvez incompletas as soluções anteriormente alcançadas pelo Direito.

Uma destas respostas adveio na forma da proteção do segredo/sigilo de informações ou dados acerca do indivíduo. Tal construção teórica baseava-se na dicotomia público-privado, de forma que se houvesse a exposição ao público de informação tida como sigilosa, ou se alguém não autorizado tivesse acesso a tais informações, estaria configurada a violação à privacidade[26].

Esta concepção de privacidade, ainda que adequada para certas situações (como, por exemplo, as previsões de inviolabilidade do lar, da correspondência, do sigilo fiscal, bancário, de informações consideradas como secretas e postas como confidenciais pela Lei de Acesso à

Volume 3 – Jan / Mar 2015. pp. 8-27. Disponível em: <https://www.ibdcivil.org.br/image/data/revista/volume3/02---rbdcivil-volume-3---o-surgimento-e-o-desenvolvimento-do-right-of-privacy-nos-estados-unidos.pdf>. Acesso em: 07 maio 2018. p. 11

[23] "Próxima do conceito anterior [do "direito a ser deixado só"], está a ideia de privacidade como o resguardo contra interferências alheias, ou seja, o "direito de o indivíduo ser deixado em paz para viver sua própria vida com um grau mínimo de interferência". Não é equivalente ao isolamento, à ausência de contato físico com terceiros, a estar longe dos outros, pois consiste na proteção do "modo de ser da pessoa, que consiste na exclusão do conhecimento de outrem de quanto se refira à pessoa mesma". A privacidade é, assim, "o direito de subtrair-se à publicidade para recolher-se na própria reserva", isto é, representa o direito de o indivíduo manter seus assuntos para si e decidir por si mesmo em que medida eles serão submetidos à observação e discussão públicas". LEONARDI, op. cit., p. 55-56

[24] "Após a II Guerra Mundial, a proteção à privacidade ganha reconhecimento no âmbito internacional. A Declaração Universal dos Direitos do Homem, de 1948, prevê, em seu art. XII, além do direito à privacidade, também o direito à honra e ao sigilo de correspondência, nos seguintes termos: *'*Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências e ataques*'*. A Convenção Européia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, o Pacto Internacional de Direitos Civis e Políticos e a Convenção Americana sobre Direitos Humanos, no Pacto de São José da Costa Rica também previram a proteção da vida privada em termos semelhantes.". MENDES, 2008, op. cit., p. 17

[25] "José Afonso da Silva destaca que prefere usar a expressão direito à privacidade, 'num sentido genérico e amplo, de modo a abarcar todas essas manifestações da esfera íntima, privada e da personalidade, que o texto constitucional (...) consagrou'". LEONARDI, op. cit., p. 80

[26] LEONARDI, op. cit., p. 62

Informação, etc), não alcança a complexidade das interações e possibilidades – mormente de violação da privacidade – permitidas pela sociedade em rede[27].

Uma outra solução encontrada para a tutela da privacidade dos indivíduos é a do controle sobre as suas informações e seus dados pessoais, mormente após o advento, democratização e popularização da computação e da internet. Nesta acepção, a privacidade seria a capacidade de o indivíduo controlar o fluxo de dados e informações a seu respeito, de revelar-se de forma seletiva ao mundo[28]. Possui profunda importância para o cenário de monetização de dados; todavia, o conceito de privacidade, restrito a esta definição, estaria defasado, sobretudo se consideradas as questões previamente abordadas.

Esta ideia de privacidade ganhou força com o julgamento, pelo Tribunal Constitucional Alemão, da lei alemã do censo de 1983[29], dando surgimento a um importante conceito para a proteção dos dados pessoais: a autodeterminação informativa[30], entendida como a prerrogativa de que dispõe o indivíduo de se resguardar contra a indiscriminada coleta e uso de seus dados e informações[31], tendo sobre eles autonomia de disposição. Tornou-se um princípio presente em diversas leis que almejam tutelar os dados pessoais e a privacidade dos indivíduos, influindo, por exemplo, na exigência imposta à determinadas companhias em informar inequivocamente ao consumidor os termos de coleta e utilização de seus dados pessoais.

Como se pôde ver, as ideias de privacidade brevemente expostas acima, apesar de suas qualidades e inegáveis contribuições para a solidificação deste direito fundamental, são incapazes de, tomadas em separado, atender às múltiplas situações de tutela e possível violação deste direito.

O "direito de estar só", e a capacidade de se "proteger contra interferências alheias" em suas esferas de intimidade[32], ainda que identificadas com o conceito (e proteção) da privacidade, não o

[27] Conceito a ser tratado com mais afinco no capítulo seguinte, mas que adianta-se como sendo uma sociedade permeada por fluxos e influxos de dados e informações, tendo estes papel preponderante na economia, que não mais é relegada a uma preconcepção em que há a separação entre produtores e consumidores estritamente distintos, havendo sim uma confusão entre estas figuras; o indivíduo passa não apenas a consumir dados e informações, mas também a produzir, tomando parte também da cadeia produtiva e participando de um círculo virtuoso de retroalimentação. Cf.: CASTELLS, Manuel. **A sociedade em rede**. Vol. 1. 8ª ed. Trad.: Roneide Venancio Majer. São Paulo: Paz e Terra, 2005.

[28] LEONARDI, op. cit., p. 68

[29] Ibidem, p 69-70.

[30] "A partir do momento em que a tecnologia passa a permitir o armazenamento e o processamento rápido e eficiente de dados pessoais, dá-se a associação entre proteção à privacidade e informações pessoais. Nesse contexto, percebe-se, uma alteração não apenas do conteúdo do direito à privacidade, mas também do seu léxico, passando a ser denominado privacidade informacional, "proteção de dados pessoais", "autodeterminação informativa", entre outros.". DONEDA, 2006, op. cit., p. 18

[31] RUARO, Regina Linden. **A tensão entre o direito fundamental à proteção de dados pessoais e o livre mercado**. REPATS, Brasília, v. 4, n. 1, p. 389-423, Jan-Jun, 2017. p. 410

[32] "A ampla aceitação desse conceito decorre, em certa medida, da popularidade da teoria das esferas, desenvolvida pelo Tribunal Constitucional alemão e esmiuçada pelas obras de Heinrich Henkel e Heinrich Hubmann. Segundo a teoria, "é possível distinguir três esferas, com intensidades de proteção decrescente: a) a esfera mais interior ('último e inviolável âmbito de liberdade humana', 'âmbito mais interno (íntimo)', 'esfera íntima inviolável', 'esfera nuclear da configuração da vida privada, protegida de forma absoluta'); b) a esfera privada ampliada, que inclui o âmbito privado que não

preenche totalmente nem o esgota. De igual maneira é a ideia de proteção de segredo ou sigilo – certamente, a proteção de dados e informações sigilosas está contida no âmbito protetivo do direito fundamental à privacidade, mas também não restringe-o à sua dimensão; exemplos existem de possível violação deste direito mesmo sem a quebra de qualquer sigilo, como os que são colocados no próximo capítulo (que trata do cenário de monetização de dados[33]), abordando o tratamento de dados públicos ou mesmo anonimizados. Isto também é verdade para o controle sobre informações e dados pessoais, apesar de coadunar-se melhor com a perspectiva sob escrutínio.

Desta forma, o direito fundamental à privacidade aparenta ter um conteúdo protetivo maleável, que se amolda e se adapta[34] a partir de contribuições da construção doutrinária e jurisprudencial[35] e, principalmente, de acordo com as necessidades e demandas da sociedade.

Assim, frente as demandas surgidas com as novas tecnologias da informação e comunicação e seus respectivos problemas[36], a privacidade como direito também apresenta novas facetas e novos contornos, almejando se encaixar neste novo cenário. Denota-se, desta constatação, o caráter contextual desse direito.

Indo além da esfera protetiva emanada pelos conceitos previamente abordados, exsurge a prática[37] da coleta de dados e informações (não apenas de dados pessoais) por empresas

---

pertence à esfera mais interior, e c) a esfera social, que inclui tudo aquilo que não for atribuído nem ao menos à esfera privada ampliada". LEONARDI, op. cit., p. 59

[33] V. g., o paradigmático caso da loja americana Target que descobriu que uma de suas clientes – uma adolescente que ainda morava com o pai – estava grávida, apenas analisando o seu histórico de compras, enviando para sua residência cupons de desconto (e uma grande dor de cabeça a um indignado pai).

[34] "privacidade seria, assim, 'um valor tão complexo e tão emaranhado em dimensões concorrentes e contraditórias, tão entupido de significados distintos e variados, que é duvidoso ser possível abordá-lo de modo útil'". LEONARDI, op. cit., p. 49

[35] "Ao tempo que Warren e Brandeis escreviam o seu tratado, entre os anos de 1889 e 1890, as intrusões da imprensa e de fotógrafos na privacidade das pessoas começaram a se tornar um fenômeno constante. […] A noção (não constitucional) de privacidade construída por Warren e Brandeis refletiu profundamente no common law a partir de então. Depois da publicação do trabalho deles, vários casos decididos pelas cortes americanas aceitaram a existência do direito à privacidade ('right to privacy')". REINALDO FILHO, Demócrito R. **Privacidade na Sociedade da Informação**. Dissertação (Mestrado em Direito). Recife: Universidade Federal de Pernambuco. 2006. p. 56-57
Danilo Doneda (2006, p. 11) faz um apanhado de casos jurisprudenciais dos primeiros processos envolvendo demandas da privacidade, demonstrando que, em sua maioria, envolviam pessoas famosas, ricas, poderosas e/ou da alta sociedade. O caso do censo alemão de 1983 também reforça este argumento, sendo exemplo mais atual as demandas judiciais envolvendo o direito ao esquecimento, tendo recentemente o STJ consolidado seu posicionamento acerca deste direito no julgamento do REsp nº 1.660.168 – RJ.

[36] "Conforme já exposto, a net revelou-se um meio propício de invasão à privacidade ao facilitar o intercâmbio de informações pessoais entre os diversos prestadores de serviço da sociedade da informação, em especial as empresas '.com'. Bancos de dados, antes off-line, integraram-se à rede, sendo transformados em bancos de dados on-line; o que implica a possibilidade de interconexão de maior número de informações pessoais identificáveis. Esses dados, conforme já exposto, são posteriormente utilizados para atividades de marketing, tais como o envio de spam ou para outros fins obscuros e não autorizados pelo titular das referidas informações". VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Dissertação (Mestrado). Brasília: UnB, 2007. 297 pp. p. 191

[37] "Data Mining. This category concerns the potential privacy threat imposed by data mining and profiling by the SNS [social network sites] provider and third parties. Since the business model of SNSs is generally based on the use of the available personal information for commercial purposes, personal data placed on these sites often becomes available for companies. The scale on which data mining occurs is reflected in the economic value of Facebook as a company […].

especializadas, redes sociais virtuais ou outros tipos de negócios, que trazem em si a potencialidade de violação da privacidade – precisamente por reunir, tratar e armazenar uma imensa quantidade de dados de diferentes origens acerca de um indivíduo ou grupo de indivíduos. Neste ponto, importa ressaltar que a autodeterminação informativa, tomada em separado[38], é incapaz de tutelar de maneira eficaz a privacidade dos indivíduos e grupos que têm seus dados pessoais coletados: isto porque, não raro, a relação entre usuário e negócios que monetizam dados pessoais se dá através de contratos de adesão, com termos determinados unilateralmente pelo provedor e nos quais o usuário pouco ou nenhum poder de barganha possui[39].

Ainda, o potencial violador do uso destes dados se encontra na capacidade de reunião de dados e informações que, mesmo que o coletor de dados tome as devidas precauções[40] para que não haja alguma invasão a seus servidores (evitando que terceiros tenham acesso aos dados, ocorrência de vazamentos, etc), ou que siga as previsões dos termos e condições de sua política de privacidade à risca (ou mesmo que não tenha sequer entabulado qualquer relação com a pessoa relacionada aos dados), pode gerar inferências acerca de aspectos íntimos da vida de quem gerou tais dados e informações.

SNSs can contain several features which affect the privacy protection of the user against data mining. First, it makes a difference whether the site owns the information posted on the site and whether information can be removed by users or remains in the database. Second, SNS generally have a policy concerning the access of third parties to personal information disclosed by the user as well". STEIJN, Wouter Martinus Petrus. The Cost of Using Facebook: Assigning Value to Privacy Protection on Social Network Sites Against Data Mining, Identity Theft, and Social Conflict. In: GUTWIRTH, Serge, et al (eds.). **Reloading Data Protection**: Multidisciplinary Insights and Contemporary Challenges. Dordrecht (Holanda): Springer, 2014. pp. 323-342 p. 325

[38] "Em razão da tremenda importância do controle sobre informações e dados pessoais, o conceito de privacidade baseado nessa ideia representa, sem dúvida, um enorme avanço. Entretanto, um enfoque exclusivo em informações e dados torna o conceito muito limitado, pois exclui certos aspectos privados que não têm relação com informações, notadamente a autodeterminação do indivíduo, isto é, o direito de uma pessoa tomar decisões fundamentais sobre sua própria vida, corpo, crenças, entre outros aspectos – na acepção do Tribunal Constitucional alemão, o direito de o indivíduo determinar autonomamente o seu destino, sem afetar direitos de terceiros, nem a lei moral, nem a ordem constitucional". LEONARDI, op. cit., p. 74

[39] "No entanto, em razão da assimetria das relações sociais e comerciais, é ilusório imaginar que o indivíduo sempre conseguirá fazer valer suas escolhas de modo significativo, quando se sabe que a ocultação de dados pessoais, ou a tentativa de controle sobre os procedimentos de coleta, processamento, uso e compartilhamento posterior desses dados, normalmente implica não poder praticar determinado ato". Ibidem, p. 78

[40] "Um exemplo relacionado à Internet ajuda a ilustrar essa situação: em 2006, o provedor norte-americano de serviços de Internet America Online publicou vinte milhões de registros, contendo as pesquisas efetuadas, ao longo de um período de três meses, por 657 mil usuários de seu mecanismo de busca. O provedor removeu todos os dados capazes de identificá-los, atribuindo a cada usuário um número aleatório. A intenção da empresa era colaborar com estudos acadêmicos. No entanto, poucos dias depois, sem maiores esforços, dois repórteres do jornal The New York Times conseguiram identificar uma pessoa, utilizando apenas os termos de busca por ela empregados, e descobriram que o 'usuário 4417749' era a Sra. Thelma Arnold, então viúva, com 62 anos de idade, residente em Lilburn, estado da Georgia, que adorava seus três cães e frequentemente buscava informações a respeito das doenças de que padeciam suas amigas. Entrevistada pelo jornal, revelou-se 'desiludida' com o ocorrido, afirmando que 'ninguém deveria ter descoberto minhas buscas', e prometeu cancelar a assinatura dos serviços oferecidos pelo provedor." Ibidem, p. 77

É o que certa doutrina chamou de "teoria do mosaico[41]": em suma, é a capacidade de, como quem monta um quebra-cabeças, formar uma figura a partir de elementos distintos e aparentemente sem conexão entre si – a figura aqui sendo a vida privada, conformada através da reunião de dados e informações. Esta devassa em potencial de aspectos íntimos da vida se dá tanto individualmente (por exemplo, o já aludido caso da loja americana *Target*[42], ou o do Facebook, que, inadvertidamente, intrometeu-se na realidade de pacientes de uma clínica psiquiátrica[43]) como coletivamente[44] (v.g., uma outra prática da *Target*, analisando o hábito de grupos de mulheres[45]).

Há ainda outras situações em que a coleta de dados pode ser potencialmente violadora da privacidade e que os conceitos unitários deste direito não alcançam ou tutelam de forma efetiva. Uma delas é o uso de *cookies* (termo técnico de informática, mais adiante abordado com maior detalhamento), nas quais páginas de internet ativamente "marcam" seus usuários ou visitantes, discriminando-os frente a enorme massa de outros navegantes da internet e, de certa maneira, conferindo-lhes elementos identificatórios. Outra situação é a coleta de dados de pessoas que sequer possuem contas em redes sociais virtuais[46], perfis ou que desejam ficar ausentes do ciberespaço

---

[41] "Nesse contexto, e em razão das deficiências da tradicional teoria das esferas para lidar com formas sofisticadas de ataque a privacidade, em sua maioria fomentadas pelo avanço tecnológico, Fulgencio Madrid Conesa propôs a alegoria do mosaico: ponderando que publico e privado sao conceitos relativos, que devem ser analisados em função de quem e o outro sujeito em uma 'relação informativa', afirma que existem dados irrelevantes a priori do ponto de vista da intimidade, mas que, em conexão com outros dados, quica igualmente irrelevantes, sob a mesma perspectiva, quando isoladamente considerados, podem servir para tornar totalmente transparente a personalidade de um individuo, 'tal como ocorre com as pequenas pedras que formam os mosaicos: em si mesmas, não dizem nada, mas unidas podem formar conjuntos plenos de significado'". Ibidem, p. 73-74

[42] HILL, Kashmir. **How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did**. Disponível em: <http://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2>. Acesso em: 01 jul. 2018.

[43] BONNINGTON, Christina. **This Is The Creepiest Facebook-Friend Suggestion Story Yet.** Disponível em: <https://www.refinery29.com/2016/08/121691/facebook-friend-suggestion-psychiatrists-office>. Acesso em: 01 jul. 2018.

WAGNER, Kurt. **Facebook's 'People You May Know' feature can be really creepy. How does it work?** Disponível em: <https://www.recode.net/2016/10/1/13079770/how-facebook-people-you-may-know-algorithm-works>. Acesso em: 01 jul. 2018**.**

[44] "Profiling can pertain to one individual person, to a group or groups of persons, but also to animals, to objects and to relations between all those. It can be used, on the one hand, to classify, describe and analyze what happened, which is not particularly new or problematic". GUTWIRTH, Serge; HILDEBRANDT, Mireille. Some Caveats on Profiling. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul (ed.). **Data Protection in a Profiled World**. Dordrecht: Springer, 2010. p. 31

[45] "More significantly, similar inferences can be made about an entire population even if only a small fraction of people who share no ties are willing to disclose. This describes the dynamics of the Target pregnancy prediction score. In this case, Target did not infer the likelihood of a woman giving birth by looking at her group of friends; rather, the company looked over the records from its baby shower registry to find women who had actively disclosed the fact that they had given birth and then went about trying to figure out if these women's shopping habits, leading up to the baby shower, seemed to differ from other customers' habits such that Target could then recognize the telltale signs in the future shopping habits of other women." TANNER, Adam. **What stays in Vegas**: the world of personal data — lifeblood of big business —and the end of privacy as we know it. New York: PublicAffairs, 2014. p. 62

[46] HASELTON, Todd. **Facebook explains how it can collect info about you even if you never post on Facebook**. Disponível em: <https://www.cnbc.com/2018/04/16/facebook-collects-data-even-when-youre-not-on-facebook.html>. Acesso em 01 jul 2018.

FRIER, Sarah. **Zuckerberg Says Facebook Collects Internet Data on Non-Users.** Disponível em: <https://www.bloomberg.com/news/articles/2018-04-11/zuckerberg-says-facebook-collects-internet-data-on-non-

(como ocorre quando, por exemplo, aplicativos de *smartphones* solicitam acesso à lista de e-mails ou da agenda telefônica).

Neste cenário de incertezas e mutabilidades – seja do conceito[47] do direito à privacidade, seja das hipóteses de sua violação – se aponta como mais seguro trabalhar com base nos fundamentos deste direito, buscando nas suas linhas mais basilares de conformação elementos norteadores que indiquem o seu conteúdo protetivo, não olvidando, por óbvio, de relacioná-lo e adequá-lo ao panorama da monetização dos dados pessoais[48] (até mesmo para manter o trabalho rente ao objetivo proposto).

Assim é que, por exemplo, alguns autores vão relacionar a privacidade como essencial à dignidade da pessoa humana, à liberdade, ao livre exercício da política[49], ao livre desenvolvimento da personalidade, à autonomia e mesmo à individualidade[50].

Stefano Rodotà[51], tratando deste direito no âmbito da sociedade em rede, explica como o aspecto "excludente" da privacidade toma uma nova roupagem, servindo de garantia à livre construção da personalidade, da identidade e aos princípios fundamentais da democracia. Para este autor, os dados pessoais conformariam uma espécie de corpo eletrônico, podendo a presença do indivíduo superar os limites de tempo e espaço, assim como sendo espécie de extensão de sua identidade. Afirma ainda que a entrega excessiva de dados pessoais poderá desembocar em uma

---

users>. Acesso em: 01 jul. 2018.

47 "Assuntos como liberdade de pensamento, controle sobre o próprio corpo, quietude do lar, recato, controle sobre informações pessoais, proteção da reputação, proteção contra buscas e investigações, desenvolvimento da personalidade, autodeterminação informativa, entre outros, são excluídos ou incluídos, de acordo com a definição adotada". LEONARDI, op. cit., p. 48

48 "Deve-se verificar como o desenvolvimento tecnológico age sobre a sociedade e, consequentemente, sobre o ordenamento jurídico; há de se considerar o seu potencial para imprimir suas próprias características ao meio sobre o qual se projeta – e não somente ressaltar as possibilidades latentes neste meio. Entra em cena, portanto, a técnica como um elemento dotado de características próprias e, consequentemente, inicia-se a discussão em torno do que seria a 'vontade de técnica'". DONEDA, 2006, op. cit., p. 16

49 "The consequences of the debate [entre privacidade e segurança] are enormous, for both privacy and security are essential interests, and the balance we strike between them affects the very foundations of our freedom and democracy". SOLOVE, Daniel J. **Nothing to hide**: the false tradeoff between privacy and security. London: Yale University, 2011. p. 1

50 "Privacy is recognized as a fundamental right in different major international legal instruments and in many national constitutions. In short, it protects a number of fundamental political values of democratic constitutional states, such as the freedom of self-determination of individuals, their right to be different, their autonomy to engage in relationships, their freedom of choice, and so on. By default privacy prohibits interferences of the state and private actors in the individuals' autonomy: it shields them off from intrusions, it provides them a certain degree of opacity and invisibility". GUTWIRTH, HILDEBRANDT, op. cit., p. 36

51 "Internet 2.0, el de las redes sociales, se ha convertido en un instrumento esencial en los procesos de socialización y en la libre construcción de la personalidad. En esta perspectiva asume un significado nuevo la libertad de expresión como elemento esencial del ser de la persona y de su situación en la sociedad. La construcción de la identidad tiende a presentarse cada vez más como un medio para la comunicación con los demás y para presentarse cada cual en la escena del mundo. Esto modifica la relación entre la esfera pública y la privada, y la noción misma de privacidad. Lo cierto es que la privacidad se construyó como un dispositivo «excluyente », como un instrumento para ahuyentar miradas no deseadas. Pero el análisis de sus definiciones muestra también sus progresivas transformaciones, que han dado lugar a un derecho que puede hacer posible la libre construcción de la personalidad, la autónoma estructuración de la identidad, la proyección en la esfera privada de principios fundamentales de la democracia". RODOTÀ, Stefano, op. cit., p. 294

realidade na qual a autonomia do comportamento humano[52] estará prejudicada, frente ao crescente uso destes dados para fins de influência nos interesses e decisões, assim como em termos de vigilância.

Em sentido similar é o pensamento do filósofo coreano radicado na Alemanha Byung-Chul Han. Ele trabalha em termos de transparência como antítese da singularidade, da individualidade: o sujeito, quando se despoja desta, seja em favor de dinheiro ou outra conformidade, cede à transparência, a qual Han tacha como sendo uma "coação sistêmica" e violenta[53]. Para este filósofo, a internet e suas ferramentas (como as redes sociais) são engendros deste sistema coator, que termina por diminuir os espaços privados, de singularidade, por uma normalização da transparência.

Combatendo essa extrapolação do público em detrimento do privado e citando Carl Schmitt, Han explicita como os aspectos obscuros, sigilosos, "arcanos", são essenciais à democracia e aos processos políticos[54], afirmando mesmo que só é inteiramente transparente o espaço despolitizado[55]. Em suma, para este filósofo, existe uma pressão sobre o indivíduo nesta quadra do século para que abandone sua individualidade e renda-se à normalização da transparência[56], agindo esta, ainda, como ferramenta de pressão que inibe a livre expressão da personalidade – aí inclusos os

[52] "La creación de este nuevo clima determina modificaciones de los comportamientos individuales que han sido descritas muchas veces y que asumen la forma de una autocensura, de una normalización «espontánea», de la adopción preventiva de comportamientos conformes al orden. En la creación de perfiles se refleja ciertamente una modelización de la sociedad que produce precisamente conformidad más que normalidad, como ya era por lo demás conocido por todos los estudiosos de los modelos culturales, cuya influencia no está en función de un valor fundamentalmente vinculante, sino del hecho de que se presentan como un paso necesario para la aceptación social en los más diversos niveles. Este efecto se amplifica y se refuerza a causa de los data mining y de los perfiles, puesto que el modelo se hace individual, se refiere a personas singulares, se utiliza de manera selectiva y escrupulosa. La aceptación social asume la forma de identidad «obligada»". RODOTÀ, Stefano, op. cit., p. 302

[53] "La coacción de la transparencia nivela al hombre mismo hasta convertirlo en un elemento funcional de un sistema. Ahí está la violencia de la transparencia". HAN, Byung-Chul. **La sociedad de la transparencia**. Trad. Raúl Gabás. Barcelona: Herder, 2013. p. 14

[54] "El «postulado del carácter público», dice Carl Schmitt, tiene «su adversario específico en la idea de que toda política lleva consigo cosas arcanas, secretos de técnica política, que de hecho son tan necesarios para el absolutismo como los secretos comerciales y empresariales para una vida económica que se basa en la propiedad privada y en la concurrencia» […] Según esto, el final de los secretos sería el final de la política. Así, Schmitt pide a la política más «valor para el secreto»". Ibidem, p. 20-21

[55] "La transparencia forzosa estabiliza muy efectivamente el sistema dado. La transparencia es en sí positiva. No mora en ella aquella negatividad que pudiera cuestionar de manera radical el sistema económico-político que está dado. Es ciega frente al afuera del sistema. Confirma y optima tan solo lo que ya existe. Por eso, la sociedad de la transparencia va de la mano de la pospolítica. Solo es por entero transparente el espacio despolitizado. La política sin referencia degenera, convirtiéndose en referendum". Ibidem, p. 22

[56] Em sentido similar também pensa Marcel Leonardi, falando mesmo em uma dimensão social da privacidade: "Isso significa que a individualidade da pessoa deve ser incorporada ao conceito de bem comum, e não entendida como seu contraponto. Quando a individualidade é separada do bem comum, o valor da privacidade diminui, e o sopesamento de princípios tende a favorecer aqueles tradicionalmente relacionados a interesses coletivos, já que os interesses sociais tendem a preponder sobre interesses individuais. É por isso que a doutrina propõe o reconhecimento de uma dimensão social da privacidade". LEONARDI, op. cit., p. 122

pensamentos ideológicos e políticos[57]. O indivíduo, segundo ele, passa a se explorar, desvalendo-se de sua individualidade em detrimento de uma transparência forçosa.

Os autores supra mencionados parecem apontar, com fundamentada razão, a privacidade como sendo um aspecto da liberdade[58]. Em retrospecto, os conceitos historicamente construídos sobre este direito aparentam se relacionar de uma forma ou de outra com certa parcela do exercício da liberdade: o direito a ser deixado só traduzia a liberdade contra intrusões, a liberdade de usufruir de solitude, de intimidades, de ter longe do público o recato do privado; o direito de resguardo contra interferências arbitrárias oriundo da Declaração Universal dos Direitos do Homem, nascida no ocaso da segunda guerra mundial e de suas atrocidades, como uma liberdade frente ao autoritarismo que desrespeitava o asilo do lar e da correspondência, e que mirava, perseguia e segregava grupos políticos oposicionistas e minorias (étnicas, religiosas e de identificação sexual diversa); a proteção do sigilo de suas informações como um direito de gerir os próprios negócios e aspectos da vida com diferentes escalas de secretismo ou publicidade; a autodeterminação informativa como a liberdade de se expor de maneira informada, inequívoca e consciente, possuindo a faculdade de não revelar-se, assim desejando; por fim, a liberdade de construir ideias e pensamentos sem o medo da reprovação de terceiros, de desenvolver sua personalidade sem censuras, de possuir seus momentos de intimidade da maneira mais aprazível possível.

Destarte, privacidade advém[59] da liberdade e subentende aspectos de liberdade, aspectos de autonomia. No âmbito da sociedade em rede, na qual os dados pessoais, sendo coletados e tratados[60], ostentam o potencial de exposição da privacidade, é de se pensar que o seu mal-uso,

---

[57] "La transparencia es un estado de simetría. La sociedad de la transparencia aspira a eliminar to das las relaciones asimétricas. También el poder pertenece a ellas. El poder no es diabólico en sí mismo. En muchos casos es productivo y generador. Genera un espacio de libertad y juego para la configuración política de la sociedad. También el poder participa en gran medida en la producción de placer. La economía libidinosa sigue una lógica de economía del poder". HAN, Byung-Chul, op. cit., p. 39-40

[58] Assim também pensa Tatiana Malta Vieira: "Privacidade e liberdade se amalgamam como duas faces de uma mesma moeda, uma vez que tão-somente o manto de proteção da privacidade proporciona a um indivíduo o direito ao exercício da liberdade. Exercer com tranquilidade a liberdade de consciência, de crença e de expressão supõe o exercício do direito que se concede a qualquer pessoa, de dispor de um espaço reservado em que possa voltar-se para si mesma, sem prender-se ao jugo de qualquer censura, sem sentir-se cativa da observação de outrem." VIEIRA, op. cit., p. 20

[59] "Os direitos da nova geração, como foram chamados, que vieram depois daqueles em que se encontraram as três correntes de idéias do nosso tempo, nascem todos dos perigos à vida, à liberdade e à segurança, provenientes do aumento do progresso tecnológico. Bastam estes três exemplos centrais do debate atual: o direito de viver em um ambiente não poluído, do qual surgiram os movimentos ecológicos que abalaram a vida política tanto dentro dos próprios Estados quanto no sistema internacional; o direito à privacidade, que é colocado em sério risco pela possibilidade que os poderes públicos têm de memorizar todos os dados relativos à vida de uma pessoa e, com isso, controlar os seus comportamentos sem que ela perceba […]" BOBBIO, Norberto. **A era dos direitos**. Trad. Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 2004. p. 96

[60] "A importância da proteção dos dados pessoais é um dos aspectos mais relevantes para o direito à privacidade. Há tempos que se reconhece que a informação, independentemente de sua espécie, converteu-se em um bem jurídico de valor extraordinário e que 'os Estados, as associações, as empresas são tão ou mais poderosas conforme disponham de grandes volumes de informação'". LEONARDI, op. cit., p. 68

descuido ou destrato possui a capacidade de violação daquele direito e, por conseguinte, de aspectos da autonomia e da liberdade do indivíduo[61].

Permite-se conjecturar, por exemplo, que os dados pessoais, conformando direta (exposição imediata de dados ou informações íntimas) ou indiretamente (pela "teoria do mosaico", e.g.) aspectos privados de indivíduos ou grupos, podem pôr em risco a liberdade[62], a autonomia e mesmo a vida destas pessoas: regimes autoritários[63], de posse de dados de oposicionistas ou dissidentes, poderiam exercer eficiente repressão; governos totalitários, sem espaço para comunidades de diferentes religiões, etnias ou orientações sexuais teriam a capacidade[64] de perseguir (e até mesmo exterminar[65]) minorias consideradas subversivas ou indesejadas.

Não se quer com esta afirmação fazer um alarde[66] à maneira de George Orwell – todavia, tampouco se mostra prudente acreditar[67] que a capacidade para tal violação não seria explorada, caso algum regime assim o quisesse. Ora, mesmo o governo da (autoproclamada) maior democracia do mundo se valeu[68] da coleta de dados e informações de cidadãos sem sequer haver suspeita ou

---

[61] "A Internet e outras tecnologias de informação podem não ter, ainda, acabado com a privacidade; no entanto, elas redefiniram o que o termo significa. Em uma era de processadores, sensores e redes extremamente baratos, a liberdade corre o risco de se tornar inversamente proporcional à eficiência dos meios disponíveis de vigilância". LEONARDI, op. cit., p. 42

[62] "a privacidade é apenas a ponta do iceberg da surveillance, pois existem outros direitos humanos violados, como a igualdade e a liberdade". MENEZES NETO, Elias Jacob de. **Surveillance, democracia e direitos humanos**: os limites do Estado na era do big data. Tese (Doutorado em Direito). São Leopoldo: UNISINOS, 2016. p. 147

[63] "De outro lado, observa-se que a privacidade, na mesma medida em que protege a liberdade, também depende dessa mesma condição para garantir a sua existência. Em regimes de repressão – como em regimes de ditadura, fascismo e nazismo – o Estado cerceia radicalmente o direito à privacidade aos cidadãos. A manutenção do poder, além da utilização de outros mecanismos, requer o controle dos pensamentos, das crenças e da expressão de toda a coletividade, sendo, portanto, medida indispensável a intromissão – velada ou ostensiva – na vida particular dos indivíduos. Não se assegura privacidade sem liberdade, e não se exercita liberdade sem privacidade". VIEIRA, op. cit., p. 21

[64] LEVIN, Sam. **Face-reading AI will be able to detect your politics and IQ, professor says**. Disponível em: <https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski>. Acesso em: 02 jul. 2018.

[65] GORTÁZAR, Naiara Galarraga. **Facebook foi crucial para limpeza étnica do século XXI em Myanmar**. Disponível em: <https://brasil.elpais.com/brasil/2018/04/12/internacional/1523553344_423934.html>. Acesso em: 02 jul. 2018.

[66] "Vale aqui reproduzir o alerta de José de Oliveira Ascensão, para quem 'instalou-se uma espécie de histeria, provavelmente de origem demagógica, na proteção de dados pessoais. As proibições multiplicam-se e excedem-se; e há particularmente um recurso desproporcionado ao direito penal. Procedendo assim, perde-se com facilidade a bússola substantiva que justifica esse regime. O que há de essencial é a defesa da personalidade. Mas as leis contentam-se com uma defesa exterior da pessoa, indiferente a valores, de modo que é o egoísmo de cada um que é realmente assegurado'". LEONARDI, op. cit., p. 76

[67] "As práticas da surveillance, auxiliadas pela tecnologia de informação, tornam visíveis mais dados ao pequeno grupo que dispõe de recursos econômicos e técnicos para processá-los. […] Sob essa perspectiva, observa-se que a prática da surveillance deve ser submetida ao controle democrático antes de se transformar em códigos de computador, ou seja, o respeito aos direitos deve anteceder todos os mecanismos de surveillance". MENEZES NETO, op. cit., p. 73

[68] Como colocado anteriormente, o denunciante americano Edward Snowden expôs as práticas da NSA (Agência Nacional de Segurança dos Estados Unidos da América) de coletar indiscriminadamente dados e informações de cidadãos americanos e estrangeiros – e até mesmo de políticos e mandatários de outras nações: "Governments also turn to data brokers and other companies to supplement their own files because the private-sector data collection is so extensive. Sometimes government agencies such as law enforcement pay for such data. In other cases, according to the NSA documents made public by Snowden, they just take it covertly. Clues to relationships, ailments, sexual orientation, religious and political affiliation, and other intimate details are easier than ever to discern, both for the private sector and for government". TANNER, op. cit., p. XV

necessidade para tanto – e o que é mais grave no âmbito de um Estado Democrático de Direito, sem a autorização de uma decisão judicial. O alerta presente no trecho que guarnece a epígrafe deste trabalho, oriundo de um trabalho da década de 1950, permanece atual: depender das dificuldades inerentes às descobertas no campo técnico para salvaguardar direitos é ainda preferível do que depender da integridade humana para tanto.

Faz-se necessário mencionar que alguns autores[69] optaram por uma concepção de privacidade pluralística, sem recorrer a um "denominador comum", a um núcleo similar que se repete em diferentes circunstâncias. Esta postura nos parece, todavia, de certa maneira enfraquecer eventuais tentativas de proteção do direito fundamental à privacidade – sobretudo considerada a imprescindibilidade de sua tutela: como proteger de forma eficiente um direito se não há uma base mínima para tanto, um ponto de partida?

É problemática levantada inclusive por Norberto Bobbio, quando alerta ser a grande questão dos direitos, na atualidade, não a sua justificação, mas a sua proteção[70]. Afirmar que um direito não tem um liame comum, que é completamente vazio, que é amplo demais para tomá-lo como certo é, ao mesmo tempo, fornecer munição aos interesses que almejam mitigá-lo, sobretudo neste cenário de utilização econômica dos dados pessoais e de riscos à privacidade.

Entretanto, tal perspectiva é válida quanto ao critério utilizado para "preencher" o núcleo mutável deste direito – é dizer, a consideração do direito à privacidade em relação aos casos concretos[71] (como já mencionado anteriormente). É viável sugerir, inclusive, que se utilize um fator

---

[69] "Afastando-se da busca por seu núcleo, propõe um conceito pluralístico, social e pragmático de privacidade, com enfoque nos problemas que precisam ser resolvidos e na utilidade social de sua tutela. Para formular sua teoria, utiliza o conceito de semelhanças de família (Familienähnlichkeit), proposto por Ludwig Wittgenstein. […] Daniel J. Solove propõe que a privacidade deve ser entendida como um conjunto de proteções contra uma pluralidade de problemas distintos, relacionados entre si. Em sua visão, esses problemas não estão relacionados por um denominador comum, ou por um elemento nuclear; cada um apresenta elementos em comum com os outros, mas não necessariamente o mesmo elemento – os problemas compartilham semelhanças de família entre si". LEONARDI, op. cit., p. 84-86

[70] "O problema fundamental em relação aos direitos do homem, hoje, não é tanto o de justificá-los, mas o de protegê-los. Trata-se de um problema não filosófico, mas político". BOBBIO, op. cit., p. 16

[71] "Não se trata de encontrar o fundamento absoluto — empreendimento sublime, porém desesperado —, mas de buscar, em cada caso concreto, os vários fundamentos possíveis. […] O problema filosófico dos direitos do homem não pode ser dissociado do estudo dos problemas históricos, sociais, econômicos, psicológicos, inerentes à sua realização: o problema dos fins não pode ser dissociado do problema dos meios". Ibidem, p. 16

base como matéria-prima neste processo: este fator base sendo a liberdade[72] que a privacidade subentende[73].

Neste azo, é possível imaginar uma analogia para ilustrar o que se propõe, baseada em termos de luz e sombra: o direito à privacidade, metamórfico, que se adapta às diferentes questões, possui não um núcleo duro, um "mínimo denominador comum" engessado, um "fundamento absoluto", como aponta Bobbio, mas sim uma *qualidade perene* que amolda-se *pari passu* ao caso concreto; esta qualidade, pelo que se afere, é a liberdade, como a sombra possui a liberdade de amoldar-se à luz de acordo com a fonte, a origem, a direção e sua intensidade – a luz aqui entendida como as potencialidades violadoras deste direito. A sombra há sempre de oscilar conforme também oscila a fonte de iluminação; de igual maneira, o aspecto da vida humana a ser tutelado pelo direito à privacidade também oscilará, sem, tampouco, perder a sua qualidade perene, que é a liberdade de modular-se. O foco da privacidade poderá cambiar – ou mesmo ser desnecessário, caso não haja luz, hipótese na qual a sombra não deixa de existir[74], mas simplesmente não se manifesta, estando latente, tal qual se comporta um direito fundamental na sua dimensão negativa[75].

Nesta lógica, quanto mais intensa e luminosa é a fonte de luz, maior e espessa também será a sombra necessária para resguardar determinado aspecto da privacidade; de igual maneira, sendo ínfima a possibilidade de sua violação originada pela emanação de um pequeno lume, minúscula ou quase inexistente também será a existência da sombra da privacidade.

É lógica que ainda abarca a própria possibilidade de mitigação deste direito, podendo efetivamente o detentor do direito à privacidade, caso assim deseje, sair do âmbito protetivo – das sombras – e ir em direção à fonte de luz, tanto o quanto assim queira, revelando-se de acordo com

---

[72] "Privacy is not merely a right possessed by individuals, but is a form of freedom built into the social structure. It is thus an issue about the common good as much as it is about individual rights. It is an issue about social architecture, about the relationships that form the structure of our society". SOLOVE, Daniel J. **The Digital Person**: technology and privacy in the information age. New York: New York University Press, 2004. p. 186
"A interdependência entre privacidade e liberdade ocorre ainda no momento em que o indivíduo invoca o seu direito à proteção da intimidade e da vida privada no que concerne ao titular desse direito decidir não apenas o que deseja expor e o que não deseja expor a respeito de si mesmo; mas também, de forma ainda mais grave, igualmente se deseja arrogar a si tal direito perante terceiros. Observa-se, portanto, que o exercício do direito à privacidade nada mais representa que o exercício do direito à liberdade, tanto a liberdade de se expor ou não quanto a de decidir em que medida pretende o titular revelar sua intimidade e sua vida privada para o mundo exterior". VIEIRA, op. cit., p. 21-22

[73] "[…] o direito à privacidade decorre do direito à liberdade, na medida em que o primeiro abriga o direito à quietude, à paz interior, à solidão e ao isolamento contra a curiosidade pública, em relação a tudo o quanto possa interessar à pessoa, impedindo que se desnude sua vida particular; enquanto o segundo resguarda o direito a uma livre escolha daquilo que o indivíduo pretende ou não expor para terceiros, protegendo o seu círculo restrito da forma como lhe aprouver". VIEIRA, op. cit., p. 22

[74] "Nesta seara, ressalta-se, ainda, o atual entendimento de que os direitos fundamentais – que visam, juridicamente, a limitar o poder estatal, proibindo a interferência no plano individual dos cidadãos e, ao mesmo tempo, exigindo uma prestação estatal efetiva para a proteção desses direitos – são autoaplicáveis no território brasileiro e, portanto, o simples fato de inexistência de legislação específica que trate do direito à proteção de dados pessoais não pode constituir óbice para que se perfectibilize a sua defesa". RUARO, Regina Linden. A tensão entre o direito fundamental à proteção de dados pessoais e o livre mercado. **REPATS**, Brasília, v. 4, n. 1, p. 389-423, Jan-Jun, 2017. p. 404

[75] VIEIRA, op. cit., p. 83

sua vontade (homenageando, desta forma, o direito à autodeterminação informativa); abarca também a mitigação ocorrida por determinação judicial, que retiraria da equação o objeto que lança a sombra tanto o quanto necessário fosse (objeto a ser entendido como o diploma legal que tutela a privacidade em cada caso concreto).

A tutela deste direito, então, resguardaria não apenas a liberdade e outros valores inerentes[76] à privacidade, mas também a liberdade (enquanto qualidade perene) deste direito de manifestar-se de acordo com o caso concreto e a necessidade de proteção.

A complexidade do tema é tanta que, mesmo diante das explanações formuladas, algo parece não situar-se firmemente; como se faltasse o aperto de um parafuso, uma "virada de chave" para a construção de uma ideia de privacidade. No intuito de suprimir esta sensação, e como defendem autores como Marcel Leonardi, Daniel Solove, Danilo Doneda e Helen Nissenbaum, é que surge a necessidade de se colocar este direito face aos casos concretos, a necessidade de contextualização. Na lógica de luz e sombra, é a necessidade de se expor o direito à potenciais riscos de violação – de incluir a luz na equação.

O trabalho, então, toma a privacidade a partir das acepções entabuladas por Danilo Doneda[77], Daniel Solove e Helen Nissenbaum[78], de forma que sua concepção depende de sua contextualização.

Na perspectiva da analogia luz-sombra, a privacidade resultaria minimamente representada face ao panorama da monetização dos dados pessoais: de um lado, a luz, representando as inúmeras vontades envolvidas e que, eventual e potencialmente, têm interesse em aspectos privados dos sujeitos de direito e ostentam a capacidade de violação dos diversos aspectos tutelados pela

[76] "First, doing so deepens our understanding of privacy and its instrumental value and at the same time highlights the distinctive ways that other ethical values are impinged and sustained, specifically, by the ways information does and does not flow. Privacy is important, in part, because it implicates these other values. Second, doing so also allows us to better formulate interventions, regulations, or remediation for the sake of these values". BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run around Anonymity and Consent. In: LANE, Julia, et al. **Privacy, Big Data, and the Public Good**: Frameworks for Engagement. New York: Cambridge University, 2014. cap. 2, pp. 44-75. p. 49

[77] "A privacidade assume, então, um caráter relacional, que deve determinar o nível de relação da própria personalidade com as outras pessoas e com o mundo exterior – pela qual a pessoa determina sua inserção e de exposição. Este processo tem como resultado o fortalecimento de uma esfera privada do indivíduo – esfera que não é a de Hubman, mas sim uma na qual seja possível a construção da individualidade e o livre desenvolvimento da personalidade sem a pressão indevida de mecanismos de controle social" DONEDA, 2006, op. cit., p. 146

[78] "Solove's taxonomy and Nissenbaum's conceptualisation, thus, provide us with a useful basis for identifying privacy issues and harms involved in surveillance activities. For the purposes of the present discussion, I suggest considering a privacy violation taking place when one of the potentially harmful actions individuated by Solove leads to a violation of contextual norms. This is the case, for instance, if data that are collected while I am surfing on the internet (i.e., while ordering plenty of junk-food) are processed to estimate the risk that I suffer or will suffer health diseases and the results are sold to health insurance companies (for instance, in order to calculate a higher health insurance premium). In these examples, an activity identified by Solove as harmful (data processing) leads to a violation of contextual norms in Nissenbaum's understanding, since I do not expect my health insurance to be informed about my purchasing habits by the (online) food store". ORRÙ, Elisa. Minimum Harm by Design: Reworking Privacy by Design to Mitigate the Risks of Surveillance. In: LEENES, Ronald, et. al. (ed.). **Data Protection and Privacy**: (In)visibilities and Infrastructures. Dordrecht: Springer, 2017. pp. 107-138. p. 120

dignidade da pessoa humana (a liberdade, em sentido amplo, o livre desenvolvimento da personalidade, liberdade política, liberdade religiosa, etc); de outro, a sombra, representando a amoldabilidade dos interesses dos sujeitos de direito (por conseguinte, também dos titulares dos dados pessoais) em se resguardar de acordo com a projeção da luz e, ao mesmo tempo, a do fator volitivo do sujeito de direito[79], que tem, nesta lógica, a faculdade de controlar sua taxa de exposição à luz ou mesmo de mitigar completamente a sombra projetada; ainda, estaria representada em tal analogia o objeto projetor da sombra, quais sejam, os diplomas legais e institutos protetores e regulatórios dos diversos interesses envolvidos.

Entendida desta maneira, a privacidade foge às críticas das acepções monistas (quando reduzida somente a um direito a estar só, ou somente ao resguardo de sigilo, etc), da redução a um direito subjetivo à privacidade (apto apenas a proteger o indivíduo e inapto a tutelar a coletividade), da busca por um "núcleo duro" e da acepção patrimonialista/contratual (limitado a uma perspectiva de reparação), logrando manter, ainda, o liame necessário com a liberdade como qualidade, tutelada e derivada de aspectos da dignidade da pessoa humana[80].

Assim estariam homenageadas, inclusive, as acepções anteriores de privacidade: a liberdade de manter-se afastado de intrusões de terceiros, de estar só; a possibilidade de manter o recato de espaços íntimos; a liberdade de manter em sigilo, tanto quanto se queira, aspectos de sua personalidade; a liberdade de orientar e influenciar, tanto quanto possível, a coleta, o uso e o fluxo de seus dados pessoais.

Cumpre ressaltar que, para este trabalho, importa a privacidade (e seus valores conexos) resultante da contextualização específica com o panorama da monetização de dados pessoais, sendo inoportunas maiores delongas quanto a contextualização da privacidade face outros cenários.

Precisamente neste âmbito da monetização de dados pessoais, o risco potencial de violação se mostra bastante alto. Como pôde-se anteriormente pincelar (e como será demonstrado no capítulo seguinte, que tratará da sociedade em rede, ciberespaço e uso de dados), a monetização dos dados pessoais oferece inúmeros riscos, tanto para os indivíduos como para grupos e coletividades.

---

[79] "[…] se o direito à privacidade pretende se constituir como espaço de livre desenvolvimento da personalidade, não se pode impedir o indivíduo de exercer livremente o direito à privacidade do qual é titular, em uma democracia constitucional, baseada na dignidade humana e na autodeterminação do indivíduo. Do contrário, correr-se-ia o risco de se ter a exclusão de direitos, liberdades e garantias em razão de um absolutismo valorativo decorrente da Constituição. O reconhecimento de que o titular do direito fundamental à privacidade tem autonomia para exercê-lo conforme os seus planos de vida e a sua vontade decorre da própria idéia de dignidade humana e do princípio da auto-determinação, que integram e moldam o cerne de todos e de cada um dos direitos fundamentais". MENDES, op. cit., 2008, p. 23

[80] "Como aspecto não finalístico, verificamos que o real interesse presente em sua tutela é o da dignidade da pessoa humana, o qual irá em última análise definir seu plano de aplicação. Neste sentido, vale a intuição de Messinetti de considerar a privacidade uma 'forma' de tutela da pessoa, antes que um valor em si". DONEDA, 2006, op. cit., p. 146

Importa salientar que os dados – precisamente os dados pessoais –, no âmbito dos modelos de negócio surgidos na esteira da sociedade em rede, funcionam como verdadeiro "fluído vital"[81]: sem eles[82], modelos tais quais a publicidade dirigida seriam infinitamente menos rentáveis. Não à toa, há quem diga que os dados são o "novo petróleo"[83], tamanha a sua abundância, sua valorização e mercantilização.

Esta analogia com o petróleo é até certo ponto precisa, sobretudo quando se considera os danos que esta matéria-prima, se manuseada de maneira descuidada ou negligente, pode causar ao meio ambiente[84], às espécies de animais em risco de extinção e à parcela da população. Comparar a exploração dos dados com a indústria de petróleo e gás é fazer um paralelo com um setor que demonstra pouca ou quase nenhuma preocupação com as consequências de suas atividades exploratórias. Sem embargo, as indústrias relacionadas ao petróleo são justa e vigorosamente reguladas, com legislações que preveem pesadas multas e sanções às companhias que violarem as regras de normatização.

Prosseguindo nesta analogia, a exploração dos dados pessoais de uma maneira desmedida, sem limites e regulações, pondo a necessidade por lucro[85] acima dos interesses da coletividade e de

---

[81] "[…] It is about how data emerged to become the lifeblood of private industry, the elixir that fuels marketing efforts to compete and expand their businesses". TANNER, op. cit., p. XIV

[82] "A informação contém em si o principal ativo da sociedade da informação, ou seja, sua principal riqueza, sendo indispensável ao desempenho de qualquer atividade – o que explica a nomenclatura atribuída pela doutrina a essa nova forma de organização social, política e econômica. O trabalho, a educação, a saúde, o lazer, a política, a economia, enfim, tudo depende de informação. Após a supervalorização da terra na época da revolução agrícola e o predomínio dos bens de produção na revolução industrial, o que prepondera agora é a informação. Na qualidade de principal matéria-prima desse novo modelo capitalista, a informação se impõe como condição determinante para o desenvolvimento econômico e cultural da sociedade, daí o intensivo uso da tecnologia da informação – enquanto mecanismo facilitador da coleta, produção, processamento, transmissão e armazenamento – o que acarreta avassaladoras mudanças no mundo". VIEIRA, op. cit., p. 157

[83] "A informação atualmente assume, diante do capitalismo, a posição que o petróleo exercia no início do século passado. Todavia, a informação não se apresenta com a pretensão de substituir velhos recursos, mas apenas alterar o antigo modo de produção de riquezas. Hoje, a linha de produção realiza-se de forma enxuta, e, particularmente, a área de marketing – pelo aumento da concorrência – requer cada mais profissionais habilitados não apenas na coleta, mas também na análise das informações, fator essencial à garantia de êxito nessa nova fase de desenvolvimento econômico. E se a informação anuncia-se o novo "petróleo", as bases de dados públicas denunciam-se como seu principal "jazigo". A iniciativa privada busca no setor público os mais diversos tipos de informação, o que faz surgir a preocupação com a necessidade de se "limitar e gerir o uso das informações" constantes nos bancos de dados públicos, sabendo-se que tais medidas produzirão reflexos diretos na economia, na política e na sociedade". Ibidem, p. 160
Algumas declarações de importantes executivos repercutiram na mídia especializada em economia, podendo-se verificar em: PRINCETON. **The world's most valuable resource is no longer oil, but data**. Disponível em: <https://www.economist.com/lealdades/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em 15 set. 2017.; VANIAN, Jonathan. **Why Data Is The New Oil**. Disponível em: <http://fortune.com/2016/07/11/data-oil-brainstorm-tech/>. Acesso em: 15 set. 2017.; e ROTELLA, Perry. **Is Data The New Oil?** Disponível em: <https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#62c474087db3>. Acesso em: 15 set. 2017.

[84] MAIA, Vinícius Fernanes Costa; XAVIER, Yanko Marcius Alencar. Relação da qualidade do Diesel brasileiro, a redução do teor de enxofre promovida pelo PROCONVE. In: XAVIER, et. al (org.). **Proteção do meio ambiente na indústria do petróleo e gás natural**. Natal: EDUFRN, 2016. p. 299-316.

[85] "Em virtude do advento das tecnologias da informação e comunicação, um outro tipo de necessidade relacionada à privacidade tem se manifestado. Trata-se da necessidade do indivíduo resguardar seus dados pessoais. Em face do valor adquirido pela informação, obtê-la tornou-se verdadeira obsessão, pouco importando se de forma lícita ou não. O fato é

direitos fundamentais – à guiza da indústria petrolífera – pode igualmente ter consequências nefastas – mormente, e como se tem mencionado ao longo do trabalho, com relação a privacidade dos titulares dos dados pessoais.

Se ousa, neste ponto, ir além e, com esteio na perspectiva da regulação do risco[86], sustentar que os dados pessoais seriam não o novo petróleo, mas, sim, o *novo urânio*, como um material radioativo. Diz-se isto em razão de o urânio, como metal radioativo extremamente perigoso, de manuseio controlado, fortemente regulado e fiscalizado, possuir uma intensa potencialidade de violação de direitos fundamentais: viola-se a liberdade de expressão, a liberdade política, científica, de credo e mesmo a liberdade econômica por meio da ameaça de bombardeamento com ogivas nucleares; viola-se potencialmente a saúde, a vida e mesmo a integridade física de futuras gerações – vide, v. g., Chernobyl ou Hiroshima e Nagasaki.

É indiscutível que o uso deste material pode gerar benefícios: tecnológicos, energéticos e mesmo bélicos. Todavia, o risco latente que ostenta o seu manuseio é altíssimo. Em sentido similar, acreditamos, é a coleta e uso dos dados pessoais: a monetização dos dados pessoais é extremamente lucrativa, mas possui riscos evidentes à privacidade[87] e, conforme defendeu-se, à liberdade.

Não custa ressaltar que a proteção dos dados pessoais, como mencionado alhures, possui mesma origem ontológica que o direito à privacidade e, por isso, falar da proteção deste direito envolve tratar da proteção dos dados pessoais[88]. Destarte, no presente trabalho, considera-se a proteção de dados pessoais como um dos aspectos advindos da contextualização do direito fundamental à privacidade no cenário de monetização de tais dados – está incluída, portanto, na ideia de privacidade.

O uso dos dados pessoais, como se mostrará ao longo do trabalho, por ter a capacidade de descortinar aspectos da privacidade e da intimidade e, ainda, ostentar potencial violador de valores e

---

que a tecnologia tem possibilitado um acesso aos dados pessoais como nunca antes, tornando possível a descoberta de aspectos relevantes da intimidade das pessoas, sem que elas ao menos se dêem conta, diante da naturalidade de se preencher uma ficha cadastral em qualquer estabelecimento médico, escolar ou comercial". SARDETO, Patricia Eliane da Rosa. **Tratamento informatizado de dados pessoais e o direito à privacidade**. Dissertação (Mestrado em Direito), Florianópolis: Universidade Federal de Santa Catarina, 2004. p. 72

[86] "A 'regulação do risco', que foi inicialmente construída para lidar com problemas de ameaças à saúde com relação a novos medicamentos, alimentos industrializados e poluição ambiental […] coloca o risco como elemento central – a incerteza quantificável […] ou a probabilidade de que um malefício vá ocorrer". ZANATTA, Rafael. **Proteção de dados pessoais como regulação do risco:** uma nova moldura teórica? In: I Encontro da Rede de Governança da Internet, 2017, Rio de Janeiro. 20 pp. p. 7

[87] "A invasão à privacidade se caracteriza ainda mais grave quando se submetem os logs registrados nos bancos de dados dos provedores à análise de agentes inteligentes, que, então, classificam os internautas em diversas categorias, conforme os assuntos pesquisados, produtos ou serviços consumidos, faixa etária, classe social e outras informações relevantes que interessem a determinados setores de publicidade ou que se destinem a qualquer outra finalidade não autorizada pela titular das informações". VIEIRA, op. cit., p. 191

[88] "O ponto fixo de referência neste processo é que, entre os prismas para enquadrar a questão, mantém-se uma constante referência objetiva a uma disciplina para os dados pessoais, que manteve o nexo de continuidade com a disciplina da privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo características próprias" DONEDA, 2006, op. cit., p. 204

liberdades conexas a este direito fundamental, encontra-se, ao que parece, incluído no conteúdo protetivo da privacidade[89]. Em síntese, para o presente trabalho, conforme argumentado, a privacidade ostenta conceituação similar àquela proposta pelos autores Danilo Doneda, Daniel Solove e Helen Nissenbaum, dependente de uma contextualização.

Assim, no decorrer desta dissertação, quando se aborda a privacidade, é tida nos seguintes termos: 1) a equação conformadora de seu conceito é *fundamentada na analogia com a metáfora de luz e sombra*, na qual a luz e seu ponto (ou pontos) de emanação são os potenciais riscos à violação da privacidade, a sombra é o conteúdo protegido por este direito e o objeto que projeta a sombra são as normas e/ou institutos que asseguram sua tutela; 2) seu liame conformador mínimo, sua qualidade perene, tal qual a característica da sombra, *é a liberdade*, aspecto fundamental da dignidade da pessoa humana, entendendo-se, assim, tanto como a liberdade a ser protegida (inerente à privacidade) como a liberdade de adaptação de sua tutela (e também de modificação/mitigação); 3) a proteção dos dados pessoais é aspecto corolário[90] da privacidade, já que o uso destes dados possui a capacidade de conformação de aspectos privados dos titulares dos dados e de potencialmente ameaçar os valores conexos à privacidade; 4) a luz (potenciais violações) se traduz nas práticas de monetização de dados pessoais, com seus respectivos riscos à liberdade e outros aspectos da dignidade (conforme se verá no capítulo seguinte); 5) os objetos que projetam a sombra são os diplomas/institutos que positivaram a tutela da privacidade e dos dados pessoais.

Dito isto, importa perscrutar os diplomas que tutelam este direito ante tal contextualização.

Dentre as constituições brasileiras, somente a Constituição de 1988 previu expressamente a inviolabilidade da privacidade e da intimidade. O Código Civil de 2002, em seu art. 21, previu também como inviolável a vida privada, estabelecendo-a no rol dos direitos da personalidade e possibilitando a reparação em caso de violação. No entanto, não há conceito para a privacidade ou rol de condutas que implicariam em sua violação.

Especificamente abordando os dados pessoais surge o art. 43 do Código de Defesa do Consumidor, lei de 1990 e que certa parte da doutrina[91] defende ser, na falta de norma que o valha,

[89] Ainda que existam posicionamentos diferentes, como o de Serge Gutwirth e Mireille Hildebrandt, que aduzem ostentar a proteção de dados pessoais uma qualidade mais ampla e abrangente que o direito à privacidade, ou como o de Dan Manolescu, que defende a existência de um direito fundamental à proteção dos dados pessoais. Cf.: GUTWIRTH; HILDEBRANDT, op. cit., p. 37; MANOLESCU, Dan. **Data protection as a fundamental right**. Effectius, Brussels, n. 5, jun./2010. Disponível em: <http://effectius.com/yahoo_site_admin/assets/docs/Data_protection_as_a_fundamental_right_Dan_Manolescu_Issue5.16761659.pdf>. Acesso em 15 jul. 2018.

[90] "Nesse contexto de desenvolvimento da tecnologia de informação, o direito à privacidade transforma-se para dar origem à disciplina da proteção de dados pessoais, de modo a se adaptar aos desafios impostos pelo avanço da técnica". MENDES, 2008, op. cit., p. 26

[91] Notadamente os professores Danilo Doneda e Laura Schertel Mendes. Conferir: DONEDA, Danilo; MENDES, Laura Schertel. Data protection in Brazil: New Developments and Current Challenges. In: GUTWIRTH, Serge, et al (eds.). **Reloading Data Protection**: Multidisciplinary Insights and Contemporary Challenges. Dordrecht (Holanda): Springer, 2014. p. 3-20.

ser lei capaz de proteger certos dados pessoais de usuários da internet em algumas ocasiões; uma vez que necessária a configuração de relação de consumo para a aplicação do referido código, não se torna, todavia, normativa abrangente o suficiente: não alcança, por exemplo, o caso dos *cookies*[92], que independe de relação de consumo para, possivelmente, violar a privacidade de um internauta.

A Lei de Acesso à Informação (Lei nº 12.527/2011), que regula o acesso a informações previsto constitucionalmente, aborda a transparência, ativa e passiva, dos entes da Administração Pública. Trouxe, na seção V do capítulo IV, previsões acerca do tratamento das *informações* pessoais – esta definição, embora pareça inexpressiva, é de extrema importância para o debate em fito, uma vez que 'informação' não deve se confundir com 'dado'[93]. Isto considerado, e em se tratando de informações de posse da Administração Pública, que as utilizam, em tese, sem fins lucrativos, queda-se inoportuna a análise desta lei em face do objetivo do trabalho.

Com maior aproximação do objeto sob exame está o Marco Civil da Internet (Lei nº 12.965/2014), que demonstrou, ao longo do seu texto, certa preocupação do legislador para com a privacidade e a proteção dos dados pessoais dos usuários da internet. Contudo, deixou a proteção destes dados à mercê da edição de lei específica – norma que, aos 14 de agosto de 2018, foi sancionada com vetos, publicada como a Lei nº 13.709/2018 – a Lei Geral de Proteção de Dados brasileira. O decreto regulador do Marco Civil (Decreto nº 8.771/2016), contudo, teve o mérito de definir o conceito de dado pessoal e procurou estabelecer certas diretrizes para a regulação de sua proteção, elencando (ainda que aparentemente eivado de atecnias) alguns entes públicos para tanto.

Vale anotar a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, por ter se originado de um vazamento de imagens íntimas da atriz homônima, e que trata da invasão/violação de dispositivos informáticos para obter, alterar ou destruir dados e informações; no âmbito do que o estudo pretende, não é, todavia, pertinente a sua análise.

Por fim, e como já adiantado, imperiosa a análise sobre a Lei nº 13.709/2018, que instituiu a LGPD no país. Apesar dos inúmeros vetos (foram onze dispositivos vetados ao todo), que recaíram, inclusive, sobre a criação da Autoridade Nacional de Proteção de Dados (espécie de agência reguladora que atuaria na fiscalização das regras atinentes ao cenário de dados pessoais no país), é a

---

[92] Assim Daniel J. Solove os define, apontando-os, ainda, como uma forma de "marcador de gado de alta tecnologia": "A cookie is a small text file of codes that is deployed into the user's computer when she downloads a web page. Websites place a unique identification code into the cookie, and the cookie is saved on the user's hard drive. When the user visits the site again, the site looks for its cookie, recognizes the user, and locates the information it collected about the user's previous surfing activity in its database. Basically, a cookie works as a form of high-tech cattle-branding.". SOLOVE, op. cit., p. 23-24.

[93] "Dado é conceituado como a representação bruta de um fenômeno, sem elaboração, ao passo que informação é o dado trabalhado, interpretado". DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Rev. Espaço Jurídico,** Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. p. 94

lei que rege, expressa e especificamente, a proteção dos dados pessoais no Brasil e, portanto, é merecedora de estudo.

A seguir, o trabalho se debruça sobre os diplomas nacionais que tutelam a privacidade – lançando a sombra que define o seu conteúdo.

2.2 CONSTITUIÇÃO FEDERAL DE 1988

Como anotado previamente, a Constituição de 1988 foi a primeira norma fundamental, no Brasil, a garantir expressamente como direito fundamental do cidadão a inviolabilidade à privacidade e à intimidade, bem como a inviolabilidade do sigilo das comunicações e dos dados, nos incisos X a XII do seu art. 5º.

A doutrina nacional debateu extensamente sobre estes dispositivos, procurando dar-lhes conteúdo[94] – uma vez que, como se viu, o constituinte não conceituou privacidade e intimidade, conferindo-lhes apenas o *status* de invioláveis. Outra problemática se deu quanto à natureza dos termos privacidade e intimidade; se seriam sinônimos ou significariam bens jurídicos distintos.

Quanto à denominação, tanto doutrina como jurisprudência parecem concordar tratarem-se de termos sinônimos[95], havendo quem estipule[96], com base na teoria das esferas, ser a privacidade uma esfera maior, estando nela inclusa a da intimidade, ambas contendo informações e aspectos da vida de um indivíduo que este considere necessário manter distante da esfera pública. Parece-nos esforço infrutífero distinguir tais termos, haja vista que, como demonstrado no item anterior, a

---

[94] "Nesse contexto, protege-se o direito à privacidade que se configura ora como norma-regra, ora como norma-princípio – a depender do caso concreto em exame. A privacidade do domicílio e a privacidade das comunicações – previstas nos incisos XI e XII do art. 5o da CF – mais se parecem com regras diante da alta densidade normativa, do baixo grau de abstração e da possibilidade de aplicação imediata. De outro lado, também se configuram como princípios ao se contatar que as garantias se estendem para além das hipóteses expressamente previstas nos dispositivos constitucionais […]" VIEIRA, op. cit., p. 63

[95] "Da mesma maneira, a Constituição Federal e o direito infraconstitucional estabelecem uma série de normas voltadas à proteção da privacidade, considerada de modo abrangente, englobando os conceitos vistos anteriormente – direito a ser deixado só, resguardo contra interferências alheias, segredo, sigilo, controle sobre informações e dados pessoais, entre outros. José Afonso da Silva destaca que prefere usar a expressão direito à privacidade, 'num sentido genérico e amplo, de modo a abarcar todas essas manifestações da esfera íntima, privada e da personalidade, que o texto constitucional (...) consagrou'. […] Nesse ponto, a distinção entre intimidade e vida privada torna-se uma discussão preponderantemente acadêmica, sem repercussão prática. Considere-se o disposto no art. 5º, X, da Constituição Federal: 'são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação'". LEONARDI, op. cit., p. 80-81

[96] "Entre os autores que preferem efetuar tais distinções, é possível verificar uma certa confusão e ausência de critérios específicos entre elas: haveria uma diferença fundamental entre os termos, e vida privada seria o mais amplo de todos; a intimidade seria 'a parte mais recôndita da privacidade, onde o cidadão pode excluir tudo e todos, sendo o mais exclusivo dos direitos, representando o direito de não ser arrastado para a ribalta contra a própria vontade'; a intimidade seria aspecto parcelar da privacidade, nos quais a reserva da atuação individual é mais intensa, abrangendo as esferas da confidência e do segredo, e como tal resguardável mesmo perante pessoas a quem não se possa opor a privacidade". Ibidem, p. 81

conformação do seu conteúdo dependerá intimamente do contexto em que encontra-se inserido, sendo o uso da expressão "privacidade" plenamente satisfatório[97].

Neste diapasão, faz mais sentido pensar a privacidade em termos amplos do que, por exemplo, limitá-la a um "direito de estar só", a um mero direito ao sigilo, ao segredo ou a um controle sobre informações e dados pessoais – sobretudo em se tratando de um direito fundamental, relacionado a vários outros valores[98].

Como já se pôde anotar, novas situações demandam novas soluções, ainda mais em um mundo cada vez mais interconectado e que testemunha a perda de preponderância do Estado[99] como único regulador e editor de normas, máxime pela capacidade das redes em superar fronteiras geográficas e, logicamente, jurisdições[100], demandando maior esforço da ciência jurídica e da jurisprudência para interpretar as previsões constitucionais de privacidade em consonância com esta realidade[101].

De toda forma, de suma importância foi a previsão do art. 5º da CF/88, que estendeu as bases[102] nas quais se deitam os demais diplomas que tutelam a privacidade.

Importa, aqui, ressaltar a previsão constitucional e fundamental da privacidade na perspectiva da analogia luz-sombra, sem o intuito de preencher seu conteúdo, mas sim denotar sua importância e dimensão; não é demais reforçar a necessidade de contextualização[103] para este

---

[97] "Por fim, pode-se dizer que a utilização do termo privacidade é adequada também pelo fato de que possui uma amplitude incomum, em comparação com os termos anteriormente mencionados, tendo sido denominada inclusive como 'palavra-ônibus' e 'noção guarda-chuva'". MENDES, 2008, op. cit., p. 20-21

[98] "A Constituição prevê diversas disposições que se relacionam à proteção da privacidade e dos dados pessoais, como a inviolabilidade da vida privada e da intimidade (art. 5º, X), a proibição da interceptação de comunicações telefônicas, telegráficas ou de dados (art 5º, XII), a vedação da invasão de domicílio (art. 5º, XI) e de correspondência (art. 5º, XII) e a possibilidade de impetração do *habeas data* (art. 5º, LXXII)". Ibidem, p. 119

[99] "Importa observar que, no decorrer do século XX, a transformação da função do Estado, aliado à revolução tecnológica, contribuiu para modificar o sentido e o alcance do direito à privacidade". Ibidem, p. 17

[100] "Um dos aspectos mais significativos e conhecidos do fenômeno da globalização é o crescente predomínio dos sistemas financeiro e econômico mundiais sobre os sistemas nacionais e locais. À medida que o livre comércio se generaliza, as disputas pelo mercado se tornam mais acirradas e as empresas transnacionais passam a atuar como sistemas integrados, os processos decisórios nacionais são submetidos a pressões desregulamentadoras […] Diante do progressivo predomínio da lógica financeira sobre a economia real, as fronteiras tendem a se tornar mais porosas, e os espaços tradicionalmente reservados ao direito e à política tendem a não mais coincidir com o espaço territorial". FARIA, José Eduardo. **Sociologia jurídica**: direito e conjuntura. 2. ed. São Paulo: Saraiva, 2010. p. 37

[101] DONEDA, 2006, p. 106

[102] "Por outro lado, a Constituição Federal brasileira estabeleceu que os direitos e as garantias nela expressos não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que o Brasil seja parte. Isso é extremamente relevante, porque a privacidade é reconhecida como um direito fundamental em praticamente todos os tratados e convenções internacionais de direitos humanos ratificados pelo Brasil.". LEONARDI, op. cit., p. 95

[103] "O inciso X do art. 5o da CF, de outro lado, mais se parece com uma norma-princípio, diante do elevado grau de abstração e generalidade, embora seja passível de aplicação direta quanto à sua parte final que prevê a possibilidade de 'indenização por dano material ou moral decorrente de sua violação'. Enfim, a análise dependerá de cada caso concreto, apresentando-se o direito à privacidade tanto como norma-regra como uma norma-princípio. Essa perspectiva é de particular importância no desenvolvimento da temática apresentada, devendo nortear os operadores técnico-jurídicos na interpretação e aplicação desse direito fundamental, em especial na resolução dos conflitos com outros preceitos constitucionais". VIEIRA, op. cit., p. 63

preenchimento. Assim, a constituição exsurge como sendo fundamental objeto projetor de sombra, conferindo à privacidade e aos valores a ela associados[104], a depender do contexto, enorme força normativa[105], atuando tanto em seu aspecto subjetivo[106] como objetivo[107].

2.3 CÓDIGO CIVIL DE 2002

O Código Civil de 2002 trouxe, no capítulo dedicado aos direitos da personalidade e expresso em seu art. 21, o direito à inviolabilidade e à reparabilidade por dano em caso de violação da vida privada da pessoa natural, garantindo, desta forma, direito à ação[108] que possa "impedir ou fazer cessar ato contrário a esta norma". Manteve um aspecto patrimonialista e individualista, "de difícil conciliação com a ordem pública constitucional, marcada por valores da solidariedade social, isonomia substancial e dignidade da pessoa humana"[109]. Confere, destarte, certa proteção à privacidade e, apesar de incorrer no mesmo vazio conceitual que a Constituição de 1988, acolhe em seu bojo valores e institutos como o nome, a imagem, os escritos, a palavra, a voz, o domicílio, a boa fama e a respeitabilidade[110].

Como se viu, a Constituição Federal e o Código Civil, ambos, atribuem certa proteção à privacidade, mas não fazem menção expressa aos dados pessoais.

---

[104] "[…] a proteção do direito à privacidade faz-se necessária à garantia de outros direitos fundamentais, tais como a liberdade de pensamento (CF, art. 5º, inciso IV); a liberdade de consciência e de crença (CF, art. 5º, inciso VI); a liberdade de expressão (CF, art. 5º, inciso IX)". Ibidem, p. 84

[105] "Constando, pois, o direito à privacidade, do rol dos direitos fundamentais, o cidadão brasileiro não se encontra totalmente desprotegido contra a violação de seus dados pessoais". SARDETO, op. cit., p. 75

[106] "Em sua dimensão subjetiva, o mesmo direito fundamental pode assumir tanto um caráter negativo como positivo. Focando-se o caráter negativo, o direito fundamental atribui ao seu titular o direito de exigir do Estado uma abstenção de intervenção na sua esfera jurídica, ou seja, impõe ao poder público o dever de não agredir a esfera jurídica do cidadão. Pelo caráter positivo, o Estado deve criar condições fáticas e jurídicas para o exercício do direito fundamental, bem como proteger seu titular de agressões provenientes de terceiros. […] A dimensão subjetiva dos direitos fundamentais corresponde à característica desses direitos de conferir ao seu titular a pretensão de exigir de alguém – do Estado e dos demais particulares – um determinado comportamento em seu favor". VIEIRA, op. cit., p. 69-70

[107] "A dimensão objetiva dos direitos fundamentais, de outro lado, significa que tais direitos representam a essência do Estado Democrático de Direito, operando tanto como limite quanto como diretriz para a atuação do poder público. Os direitos fundamentais, em sua dimensão objetiva, representam os valores a serem perseguidos pelo Estado, porque representam a base de todo o ordenamento jurídico". Ibidem, p. 70

[108] O Google, em petição ao Supremo Tribunal Federal criticando o "direito ao esquecimento" (em poucas palavras, o direito a ter retirado ou desindexado da web conteúdos sobre si), afirmou ser o Brasil o segundo país que mais emite ordens judiciais para a retirada de conteúdo, perdendo apenas para a Rússia. Desde 2009, das 5.261 solicitações para remoção de conteúdo, 189 têm como motivo a difamação e 124 a privacidade/segurança. Para mais informações, conferir: LUCHETE, Felipe. **Brasil é segundo país que mais manda Google apagar conteúdo da internet**. Disponível em; <http://www.conjur.com.br/2017-set-09/brasil-pais-manda-google-tirar-conteudo-internet>. Acesso em: 10 set. 2017. Para ler a petição do Google: <https://goo.gl/e2WgqS> (RE 1.010.606).

[109] LEONARDI, op. cit., p. 94

[110] KLEE, op. cit., p. 127

Vale mencionar que, quando se relaciona dados pessoais à privacidade, mormente considerando as previsões constitucionais, é preciso ter em mente duas situações[111]: a de transmissão de dados e a da coleta, armazenamento e tratamento de dados.

Na transmissão de dados, têm-se que são invioláveis, só podendo ter o seu sigilo quebrado mediante ordem judicial. A analogia da correspondência é pedagógica: se alguém envia uma carta, selada, para outrem, ambos (quem envia e quem recebe) têm a expectativa de que sua comunicação permaneça intacta; a violação de correspondência, inclusive, tem previsão cominativa no Código Penal, no art. 151.

De maneira similar, as conversas telefônicas, telemáticas e a transmissão de dados possuem tutela (inclusive constitucional) quanto à sua inviolabilidade. A privacidade, nesta situação, é mais palpável, vez que expressa no conteúdo destas transmissões. Não à toa, certos serviços de mensagens, como o *WhatsApp*, adotaram a criptografia ponta-a-ponta[112], na qual o servidor, simples "mensageiro", não tem acesso ao conteúdo das mensagens.

De outra banda, a coleta, armazenamento e tratamento de dados pessoais requer um entendimento que apenas o atual cenário da sociedade informacional pode proporcionar. No mundo analógico, com arquivos em folhas de papel, separados entre si, a correlação de dados e informações era trabalho demorado e custoso. Na sociedade em rede, com a digitalização dos dados e a possibilidade de seu correlacionamento e tratamento, tornou-se mais fácil retirar significado da conjugação de bases de dados diversas[113].

É instrutiva essa distinção entre o período analógico e o digital; pense-se no trabalho de um detetive: em tempos idos, o trabalho de um investigador para fazer uma devassa na vida de determinado indivíduo era mais complexo, demandando muitas horas de trabalho e acesso a inúmeros arquivos, fichários e almoxarifados de entes públicos.

No ciberespaço, o que levaria talvez centenas de horas para um detetive, pode ser realizado em segundos por um algoritmo ou outra solução de *big data* (sem tradução específica, é um termo que pode ser entendido como representante de um cenário contenedor de uma vasta gama de dados disponíveis). O detetive, agora, se torna um "Sherlock 2.0": a partir de pedaços de dados aparentemente distintos, destoantes e desconexos, um algoritmo é capaz de deduzir comportamentos, gostos, preferências, itinerários e uma série de outras informações. Monta-se um quebra-cabeças que, a partir de peças diferentes, faz surgir uma figura compreensiva sobre

---

[111] MARCACINI, Augusto Tavares Rosa. **Direito e Informática**: uma abordagem jurídica sobre a criptografia. Rio de Janeiro: Forense, 2002. p. 146

[112] WHATSAPP. **Criptografia de ponta-a-ponta**. Disponível em: <https://faq.whatsapp.com/pt_br/android/28030015/>. Acesso em: 07 jul. 2018.

[113] LEONARDI, 2011, p. 68

determinado indivíduo. É a teoria do mosaico em ação, como prefere a doutrina mencionada previamente.

Assim, a conformação e possível violação privacidade, como se vê, depende da coleta, armazenamento e tratamento de dados pessoais. Exemplo disto é o já aludido caso do pai que descobriu que seria avô porque uma loja varejista enviou para sua residência, endereçados a sua filha, cupons de desconto para produtos relacionados à gravidez e bebês.

Por fim, tem-se que o Código Civil confere a possibilidade de reparação face à violação de aspectos da privacidade do sujeito de direitos, seja na transmissão de dados, seja na coleta de dados, ostentando uma natureza de direito remedial[114].

Como bem apontado por Danilo Doneda, a esta classificação de direito falta o ferramental capaz de ativamente proteger o sujeito de direito – um aspecto promocional – vindo a atuar somente quando o dano já ocorreu. Não deixa de ser, apesar disso, importante diploma, vez que a possibilidade de se ajuizar ação reparatória pode atuar como fator desencorajante aos que, eventualmente, estejam projetando luz em aspectos privados dos sujeitos sem os devidos resguardos.

Não obstante, entendemos que, ante a especificidade do Marco Civil da Internet, seu decreto regulador e da Lei Geral de Proteção de Dados, no escopo do objeto estudado, a aplicação do Código Civil resta subsidiária.

2.4 TUTELA DA PRIVACIDADE EM OUTROS DIPLOMAS INFRACONSTITUCIONAIS

2.4.1 Código de Defesa do Consumidor (Lei nº 8.078/90)

Elenca-se o Código de Defesa do Consumidor em razão de seus artigos 43 e 44, que abordam os bancos de dados e cadastros de consumidores. Mais específico para a proteção dos dados pessoais é o art. 43, expondo que o consumidor terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as

[114] "A tutela remedial, típica do direito subjetivo, não é mais do que um dos instrumentos entre outros a serem utilizados para a tutela da privacidade, e de forma alguma é a estrutura na qual deva moldar-se. A ela faltam os instrumentos adequados à realização da função promocional da tutela da privacidade como meio de proteção da pessoa humana e da atuação da cláusula geral da proteção da personalidade; nela igualmente não é concebida a dimensão coletiva na qual se insere a problemática da privacidade. Neste sentido deve ser entendida a tutela da privacidade através da responsabilidade civil que, se é uma perspectiva que não deve ser descartada como opção para uma série de situações, por si só não promove um avanço na tutela oferecida pelo ordenamento em relação à privacidade. Nesta perspectiva, ela continuaria a ser encarada como mera liberdade negativa, isto é, desconsiderando tanto a evolução da matéria como o alcance da norma constitucional, que ao considerar a privacidade em seu aspecto positivo, destaca sua função promocional – para o que deve lançar mão de outros institutos". DONEDA, 2006, op. cit., p. 143-144

suas respectivas fontes. Deve-se fazer a ressalva, todavia, que este diploma legal atuará na forma do art. 4º, III; qual seja, tutelará apenas as situações que configurarem relações de consumo.

Muitas das redes sociais virtuais[115] exigem, bem como outros serviços (provedores de e-mail, de armazenamento na nuvem e de *streaming* de músicas e vídeos), quando do cadastro de usuários, a anuência destes a termos de uso e políticas de privacidade[116], nos quais estão contidas as disposições acerca da coleta, armazenamento, uso, tratamento e finalidade dos dados pessoais. Neste momento de cadastro, ocorre uma contratação[117] entre o provedor do serviço e o usuário, inexistindo, na esmagadora maioria das vezes (vide os termos do *Facebook* e do *WhatsApp*, por exemplo) possibilidade de o usuário modificar ou questionar cláusulas destes termos, explicitando a posição de vulnerabilidade do consumidor em tais relações[118]. Diz-se, então, que há o avençamento de um contrato de adesão, conforme definido no art. 54 do CDC[119].

Assim, em se caracterizando uma relação de consumo, aplicável os ditames do art. 43 do CDC[120], mas há quem defenda que este diploma, por estabelecer um conceito amplo de consumidor, poderia ser aplicado em outros casos além daqueles em que há estrita relação de consumo[121].

---

[115] Definindo este tipo de serviço, Chiara Spadaccini de Teffé e Maria Celina Bodin de Moraes afirmam que "as redes sociais têm em comum as seguintes características: i) a existência de um ambiente propício à interação entre os usuários na plataforma; ii) o pedido de dados pessoais para a criação de perfis, que são vinculados a contas determinadas; iii) a articulação de uma lista de outros usuários com os quais se compartilha conexões; e iv) o oferecimento de ferramentas que permitem e estimulam que o usuário adicione seu próprio conteúdo na rede, como fotografias, comentários, músicas, vídeos ou links para outros sites, de modo que ocorra a expansão da estrutura da própria rede social" TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar**, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017. p. 117.

[116] "Ainda que, na prática, tais políticas apresentem redação excessivamente genérica e sirvam como mero aviso de que o titular do Web site coletará as informações que desejar e fará com elas o que bem entender, o fato é que representam um pequeno avanço, possibilitando aos usuários saber – caso leiam o documento – o que será feito com suas informações pessoais ao utilizar determinado Web site ou contratar com aquele fornecedor, o que não ocorre com outros meios de contratação à distância, principalmente pelo telefone. Em última análise, porém, caso a política de privacidade adotada pelo Web site não pareça satisfatória, ao usuário restará apenas não utilizar o serviço ou deixar de contratar com aquele fornecedor". LEONARDI, op. cit., p. 207-208

[117] "Boa parte dos procedimentos de coleta, armazenamento e processamento de dados pessoais no âmbito da Internet ocorre em decorrência de uma relação de consumo entre um provedor de serviços (fornecedor) e um usuário (consumidor)". Ibidem, p. 198

[118] "O princípio da vulnerabilidade é um dos mais relevantes consagrados pelo Código, na medida em que consiste no reconhecimento do estado de risco e fragilidade do sujeito de direitos inserido no mercado de consumo. É a partir desse reconhecimento que o Código de Defesa do Consumidor é capaz de estabelecer um regime diferenciado para reequilibrar os poderes na relação de consumo". MENDES, 2008, op. cit., p. 129

[119] Art. 54. Contrato de adesão é aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo. BRASIL. **Código de Defesa do Consumidor**. Lei 8.078, de 11 de setembro de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/l8078.htm>. Acesso em: 07 jul. 2018.

[120] KLEE, Antonia Espíndola Longoni. A regulamentação do uso da internet no Brasil pela Lei nº 12.965/2014 e a proteção dos dados e dos registros pessoais. **Direito & Justiça**, Porto Alegre, v. 41, n. 2, p. 126-153, jul.-dez. 2015. p. 132; RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. **Revista da Faculdade de Direito** - UFPR, Curitiba, n. 47, p.29-64, 2011. p. 60

[121] DONEDA; MENDES, op. cit., p. 7-8

Os parágrafos do referido artigo[122] dispõem sobre como devem ser os bancos de dados mantidos por quem os coleta. Neste azo, os cadastros devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos; deve haver comunicação quando da abertura de cadastro, ficha, registro e dados pessoais e de consumo quando o consumidor não o solicitar; pode o consumidor, encontrando inexatidão nos seus dados e cadastros, exigir sua imediata correção; e o acesso a tais dados devem ser disponibilizados em formatos acessíveis, inclusive para a pessoa com deficiência.

Para Danilo Doneda e Laura Schertel Mendes, quatro pilares do microssistema consumerista seriam de utilidade na promoção e salvaguarda dos dados pessoais: primeiro, regulações específicas sobre banco de dados, abordando procedimentos de retificação e aviso; segundo, uma cláusula ampla regulando a reparação por danos, a partir da responsabilidade objetiva; terceiro, uma estrutura pública de auxílio ao consumidor (como a existência de PROCON's e Juizados Especiais) e; quarto, um conceito extenso de consumidor[123]. Todavia, e como estes mesmos autores explicam, há situações as quais a proteção e os princípios previstos no CDC não alcançam no paradigma da sociedade informacional[124].

O exemplo dos *cookies*[125] é ilustrativo para o que se afirma. Criados pelos sites visitados *online*, os *cookies* armazenam informações sobre o visitante e como ele utiliza o site no dispositivo de acesso[126] – seja ele o computador pessoal, o notebook, *smartfones* ou outro dispositivo. Eles guardam dados sobre o usuário, rastreando, por exemplo, seus movimentos e padrões de uso, sendo esta prática muito utilizada na publicidade dirigida.

[122] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. BRASIL. **Código de Defesa do Consumidor**. Lei 8.078, de 11 de setembro de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/l8078.htm>. Acesso em: 07 jul. 2018.

[123] DONEDA; MENDES, op. cit., p. 7

[124] "First of all, problems related to data protection in the Internet need a special attention of the regulators. Problems concerning data protection in social networks, cookies, behavioral advertising, cloud computing as well as problems related to privacy on smart phones demand a specific approach. It is clear that these are all transnational problems, and as such they need a supranational response.". Ibidem, p. 17

[125] Em retrospecto: "A cookie is a small text file of codes that is deployed into the user's computer when she downloads a web page. Websites place a unique identification code into the cookie, and the cookie is saved on the user's hard drive. When the user visits the site again, the site looks for its cookie, recognizes the user, and locates the information it collected about the user's previous surfing activity in its database. Basically, a cookie works as a form of high-tech cattle-branding.". SOLOVE, 2004, op. cit., p. 23-24

[126] CHERRY, Denny. **Fundamentos da privacidade digital**. Rio de Janeiro: Elsevier, 2015. p. 7

Como se vê, os *cookies* são arquivos criados pela simples visita a um site. Inexiste, no simples acessar de uma página, uma relação de consumo, mas existe, sim, a potencialidade de acesso a dados pessoais do usuário e, portanto, algum grau de possibilidade de violação da privacidade[127].

Em resumo, pode-se dizer que, em se tratando de situações que configurem relações de consumo ou, pela doutrina referida (com uma posição que confere mais abrangência aos dispositivos do CDC), havendo hipótese que recaia de alguma maneira nas disposições do art. 43 do CDC, este diploma pode ser invocado na proteção de dados pessoais[128] e, consequentemente, no resguardo à privacidade. Importante ressaltar, contudo, a complexidade[129] das relações vivenciadas e proporcionadas pela internet que o CDC, infelizmente, não alcança[130].

2.4.2 Marco Civil da Internet (Lei nº 12.965/2014)

A Lei nº 12.965/2014, que ficou conhecida como Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Com um processo legislativo democrático e plural[131], tendo sido realizadas diversas chamadas públicas e tendo-se ouvido entes da sociedade civil, especialistas em informática, em direito digital e entes do terceiro setor, é uma lei modelo, principiológica e de caráter amplo[132].

Nesta norma, o termo "privacidade" aparece quatro vezes; "intimidade", cinco; "vida privada", três e, dados pessoais, onze. Em um universo de 32 artigos, cinco dos quais dedicados às

---

[127] VIEIRA, op. cit., p. 194

[128] "Ao se examinar o tratamento de dados pessoais realizado no âmbito da relação de consumo, é fundamental se considerar a vulnerabilidade do consumidor nesse processo. Isso porque, os dados pessoais, assim como as demais informações extraídas a partir deles, constituem-se em uma representação virtual da pessoa perante a sociedade, ampliando ou reduzindo as suas oportunidades no mercado, conforme a sua utilização". MENDES, 2008, op. cit., p. 129

[129] "É preciso compreender que os problemas relativos à coleta e ao uso de informações armazenadas em bancos de dados e cadastros de consumo são muito distintos daqueles relacionados às práticas de vigilância governamental. A surrada metáfora de uma sociedade de controle, baseada na obra 1984, de George Orwell, não é útil para a compreensão dessas questões. Isso porque a metáfora de Orwell tem como escopo os danos causados pela vigilância – a inibição de comportamentos e o controle social – e não os danos causados pelo processamento de informações – seu armazenamento, sua utilização e sua análise. O "Grande Irmão" visualiza um poder autoritário centralizado que objetiva um controle absoluto, mas os dossiês digitais construídos pelas empresas não são controlados por um poder central, e seu objetivo não é oprimir, mas sim estimular o consumo". LEONARDI, op. cit., p. 203

[130] "O principal problema dos dossiês digitais é possibilitar, por meio da agregação de dados antes esparsos, a criação de perfis completos de consumidores e a prática de dataveillance, definida por Roger Clarke como "o sistemático uso de sistemas de dados pessoais na investigação ou monitoramento das ações ou comunicações de uma ou mais pessoas. […] O risco de o consumidor ser considerado incapaz de contratar ou de honrar seus compromissos, com base em meros fragmentos de informações, é enorme. É nesse contexto que se percebe a insuficiência da tutela prevista no Código de Defesa do Consumidor para lidar com os problemas trazidos pelos dossiês digitais". Ibidem p. 203-204

[131] LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 4-5

[132] ZANATTA, Rafael A. F. A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet, in: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. **Direito e Internet III**: Marco Civil da Internet. São Paulo: Quartier Latin, 2015, p. 447-470. p. 462

disposições finais, é perceptível a importância[133] que o legislador conferiu à proteção do direito à privacidade.

Seu art. 2º elenca como fundamentos à disciplina do uso da internet no Brasil o respeito aos direitos humanos, ao desenvolvimento da personalidade e ao exercício da cidadania em meios digitais (II); assim como à livre iniciativa, à livre concorrência e à defesa do consumidor (V). Sendo direito fundamental previsto constitucionalmente e direito humano previsto na Declaração Universal dos Direitos Humanos em seu art. XII[134], a privacidade encontra-se, portanto, aludida no inciso II; o inciso V é de suma importância, uma vez que, ao mesmo passo em que elenca a livre iniciativa (em dispositivo posterior correlacionada com a liberdade de modelos de negócio – aí inclusos os que utilizam dados pessoais) como fundamento, também prevê a proteção do consumidor e seus direitos.

O art. 3º estabelece os princípios do uso da internet. Para a presente análise, pertinentes o inciso II, prevendo a proteção da privacidade; o inciso III, prevendo a proteção dos dados pessoais, na forma da lei; o inciso V, determinando a preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; e a liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta lei, em seu inciso VIII.

O inciso II é expresso e explícito: a proteção à privacidade é princípio informador na interpretação das relações dadas no âmbito do uso da internet. Sua violação é, portanto, defesa. O inciso seguinte prevê a proteção dos dados pessoais, mas a condiciona à edição de lei específica, recentemente publicada sob o nº 13.709/2018. O inciso V, prevendo a utilização de boas práticas para a manutenção da segurança da rede, indiretamente prevê a utilização das técnicas mais avançadas no sentido de proteger os usuários (a exemplo da criptografia, da privacidade por design, entre outros aspectos).

Por fim, o inciso VIII, dialogando com o inciso V do art. 2º, permite a liberdade dos modelos de negócio promovidos no ciberespaço, fazendo a ressalva de que não conflitem com outros princípios previstos no Marco Civil: isto considerado, parece clara a intenção do legislador

---

[133] "Em vista da importância do assunto, o Marco Civil estipulou a privacidade e proteção dos dados pessoais como princípios fundamentais, em seu artigo 3º, incisos II e III, trazendo como direito e garantia dos usuários a necessidade, em regra, de seu consentimento livre, expresso e informado, para a coleta, o uso, tratamento ou armazenamento dessas informações, diante das previsões, também, do artigo 7º, VIII e IX,13 do Marco Civil […]". LIMA, Caio César Carvalho. Garantia da privacidade e dados pessoais à luz do marco civil da internet. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 152

[134] XII - Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques

ao estabelecer, inclusive numericamente anterior, o disposto nos incisos II e III do art. 3º (proteção da privacidade e dos dados pessoais).

O art. 7º, por sua vez e em atinência ao objeto do presente estudo, assegura os seguintes direitos aos usuários da internet: sem eu inciso I, a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; inciso II, a inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; inciso III, inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial. O inciso primeiro, claro e conciso, prescinde de interpretação, e referendando o apontamento feito ao fim do tópico 2.3 deste trabalho surgem os incisos II e III: o legislador protegeu os dois momentos nos quais há a possibilidade de violação da privacidade dos usuários – a partir do fluxo dos dados e da coleta e armazenamento destes.

O inciso VI, à guiza das disposições do CDC, prevê a obrigação de fornecimento de informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade. Dispositivo seguinte prevê, ainda, obrigação quanto à responsabilidade no trato dos dados pessoais, vedando o fornecimento a terceiros de dados pessoais, inclusive registros de conexão e de acesso a aplicações de internet, a não ser que haja consentimento livre, expresso e informado ou nas hipóteses previstas em lei; neste último trecho, o legislador consagrou o direito da autodeterminação informativa, definido por Regina Linden Ruaro[135] como "o direito que tem o indivíduo de escolher com quem pretende compartilhar suas informações, partindo do pressuposto de que pode vetar qualquer ingerência não consentida". Seguindo o mesmo raciocínio são os incisos VIII, IX, X e XI[136].

O inciso XIII reforça a aplicação do microssistema consumerista nas relações de consumo realizadas na internet. Arrematando o rol de direitos, o art. 8º prevê como condição para o pleno exercício do direito de acesso à internet a garantia do direito à privacidade, estabelecendo como nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como as que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet (inciso I).

---

[135] Op. cit., 2015, p. 45

[136] VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

A seção II, compreendendo os arts. 10 a 17, disciplina a proteção dos registros, dos dados pessoais, das comunicações privadas e da guarda dos registros de conexão tanto de provedores de conexão como de aplicativos[137].

Pela leitura do art. 10º, têm-se que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas, revelando, uma vez mais, a preocupação que teve o legislador no resguardo dos direitos dos usuários, mormente do direito fundamental à privacidade[138]. Os parágrafos 1º e 2º, orientados pelos ditames constitucionais, previram como regra a necessidade de ordem judicial para a disponibilização dos registros e das comunicações privadas; o § 4º segue o direito da autodeterminação afirmativa quanto à clareza sobre os processos de segurança na proteção dos dados pessoais.

Assim, percebe-se que estas características, na acepção de privacidade adotada neste trabalho, incluem-se na sombra de conteúdo projetada pelo Marco Civil, na medida em que a sua potencial violação exporia aspectos privados dos sujeitos de direito e a liberdade deles advinda. Registros de conexão e acesso já são pleiteados na justiça por figuras políticas que desejam superar a anonimização permitida pela internet na busca por identificar seus críticos[139], pondo em xeque, de tal maneira, a liberdade de pensamento, de expressão e a liberdade política.

---

[137] Provedores de conexão (na intelecção do art. 9º do Marco Civil da Internet) são aqueles que provêem conexão à Internet, que fornecem o fluxo de dados que permitem o acesso à rede mundial de computadores; são provedores de conexão, por exemplo, a NET e a GVT; TIM, Claro e Vivo são exemplos de provedores para dispositivos móveis (em redes 3 e 4G). Já os provedores de aplicação são conceituados no art. 5º, VII, do Marco Civil da Internet como um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; exemplo deles são o Google, o Facebook, Outlook, Twitter, entre tantos outros dos incontáveis serviços e aplicações oferecidos online.

[138] "Para que se consiga melhor compreender o tema da garantia e da proteção de dados pessoais, importante entender e distinguir os principais tipos de registros eletrônicos referidos na Lei 12.965: registros de conexão; registros de acesso a aplicações; dados pessoais; e o conteúdo das comunicações privadas. Os conceitos de registros de conexão e de acesso a aplicações são bastante semelhantes e estão explícitos no próprio Marco Civil. Englobam as informações de início e término das conexões ou de uso de determinada aplicação, incluindo o número de Protocolo da Internet (IP - *Internet Protocol*) vinculado, com informação de data, hora, minuto e segundo de conexão ou acesso". LIMA, op. cit., p.153

[139] MARCHETTI, Brunno. **Alckmin acionou Justiça para descobrir IP de quem o xingou muito no twitter**. Disponível em: <https://motherboard.vice.com/pt_br/article/78wzv9/alckmin-acionou-justica-para-descobrir-ip-de-quem-o-xingou-muito-no-twitter>. Acesso em 08 jul. 2018.

SILVA, Marcos Sergio. **Juiz dribla Marco Civil e dá a Doria direito de identificar críticos no Facebook**. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2017/04/21/juiz-dribla-marco-civil-e-da-a-doria-direito-de-identificar-criticos-no-facebook.htm>. Acesso em 08 jul. 2018.

O art. 11 e seus parágrafos[140] se relacionam com o já alertado anteriormente por José Eduardo Farias, Danilo Doneda e Laura Schertel Mendes, quanto ao caráter descentralizado, supranacional e superador de barreiras geográficas da internet, ensejador de complexidades e novos imbróglios.

Traduzindo-se em um esforço do legislador para superar estes desafios, o referido dispositivo estabeleceu que, em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet, nas quais pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Assim é que, por exemplo, se um brasileiro acessa ao *Facebook*, com servidores físicos baseados nos Estados Unidos, a partir de um computador ou *smartphone* situado no Brasil, o Marco Civil surge como eventual projetor de sombra, de conformador de conteúdo tutelado pela privacidade.

Os arts. 13 a 17 tratam da guarda de registros, sejam de conexão, de acesso a aplicações de internet na provisão de conexão ou de aplicações. Encontram sua definição no art. 5º, incisos VI e VIII. Assim, o registro de conexão é o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados; e o registro de acesso a aplicações de internet, o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Disciplinam a forma que deve se dar a guarda (manutenção em segurança e guardando sigilo), determinam a responsabilidade pela manutenção dos mesmos, quem será o responsável (administrador de sistema autônomo ou pessoa jurídica que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos), prevendo ainda a possibilidade de

[140] § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

requisição por autoridades (policial, administrativa ou mesmo o Ministério Público[141]) e sanções em caso de descumprimento.

Merece destaque, para os fins deste trabalho, o art. 16, que dispõe, na provisão de aplicações de internet, onerosa ou gratuita, a vedação da guarda dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º (inciso I) ou de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular (inciso II).

Percebe-se, destarte, a importância conferida pelo legislador à autodeterminação informativa e ao consentimento nas relações dadas no âmbito da internet, estabelecendo fundamentação legal à necessidade de transparência, conscientização, ética e mesmo boa-fé das empresas que utilizam os dados pessoais e a privacidade dos usuários em seus modelos de negócio[142].

Entretanto, e como se viu anteriormente, pela complexidade e variedade das situações surgidas com o advento da sociedade em rede, "é ilusório" pensar que a panacéia para os problemas jurídicos advindos neste novo paradigma se encontrem todos nesta lei[143], sendo premente a edição de lei específica para a proteção dos dados pessoais na busca pela efetivação da privacidade (como condição *sine qua non* do uso pleno da internet).

2.4.3 Decreto nº 8.771/2016

O decreto regulador do Marco Civil (Decreto nº 8.771/2016) trata das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indica procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, aponta medidas de transparência na requisição de dados cadastrais pela administração pública e estabelece parâmetros para fiscalização e apuração de infrações. Foi sancionado na intenção de preencher certo vácuo normativo demandado pelas disposições do Marco Civil.

[141] Victor Hugo Pereira Gonçalves critica esta disposição: "As preocupações com a falta de quais informações deverão ser guardadas pelo Provedor de Aplicações, quem é esse Provedor de Aplicações e o tempo excessivo de seis meses estipulado pelo *caput* do art. 15 exponenciam-se no § 2o. Os desvios interpretativos possíveis serão muito mais discricionários com a liberalidade de se outorgar à autoridade policial ou administrativa e ao Ministério Público o direito de requererem informações sobre os usuários, sem prazo determinado. É o Estado de Vigilância desenhado no *caput* que se realiza no § 2o. Não haverão limites legais impostos aos mecanismos estatais de investigação para defender os usuários do vigilantismo e dos desvios à sua privacidade. No contexto do Marco Civil não há ferramentas, normativas ou digitais, estipuladas para que o usuário tenha acesso ao conteúdo das informações produzidas e guardadas por essas autoridades, cujo prazo é indefinido. A proteção deficiente é um meio de obstrução de direitos e garantias constitucionais de onde o arbítrio se oxigena para expandir os seus espaços. O Marco Civil, no § 2o do art. 15, é porta de entrada para uma série de possibilidades que não estariam no escopo inicial do projeto participativo, construído socialmente. O discurso de busca de igualdade social não se vê espelhado no texto desse artigo, que se distancia das lutas que ensejaram esta 'constituição' da internet.". GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado**. 1. ed. São Paulo: Atlas, 2017. p. 86

[142] ZANATTA, 2015, op. cit., p. 467

[143] Ibidem, p. 462

De relevância para a análise em escopo são os arts. 11 a 16, abordando a proteção e os padrões de segurança e sigilo dos registros, dos dados pessoais e das comunicações privadas.

Quanto as autoridades administrativas previstas no art. 10 do Marco Civil, determina o art. 11 a obrigação de indicar a fundamentação legal e a motivação para o acesso aos dados cadastrais de usuários, definindo ainda o que são os dados cadastrais: a filiação, o endereço, a qualificação pessoal (nome, prenome, estado civil e profissão). O art. 12[144] prevê, ainda, o dever de transparência na contabilização destes pedidos de acesso por parte das autoridades administrativas.

Do art. 13, de suma importância a intelecção do inciso IV, que determina, para os provedores de conexão e de aplicações em hipóteses de guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, a adoção de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes. Assim, de posse dos dados pessoais ou informações que de alguma forma violem a privacidade do usuário, o provedor de conexão e aplicação tem o dever de tomar todas as medidas possíveis para a salvaguarda deste direito fundamental. Exemplo disto foi a adoção, pelo aplicativo *WhatsApp*, da criptografia "ponta-a-ponta"[145].

O art. 14 teve o mérito de definir tanto dado pessoal como o processo de tratamento de dados pessoais[146]; o art. 15 preleciona, fazendo menção ao art. 11[147] do Marco Civil, a necessidade de estruturação e interoperabilidade dos dados que passem por coleta, armazenamento, guarda ou tratamento em território nacional, para facilitar seu acesso caso sejam alvo de decisão judicial ou solicitação por autoridade administrativa. O art. 16, por fim, determina o dever de clareza e acessibilidade, para com qualquer interessado, sobre os padrões de segurança adotados para proteger os dados pessoais.

A problemática deste Decreto, todavia, encontra-se nos arts. finais (17 a 21), que distribui competências quanto à fiscalização e transparência.

---

[144] Art. 12. A autoridade máxima de cada órgão da administração pública federal publicará anualmente em seu sítio na internet relatórios estatísticos de requisição de dados cadastrais, contendo: I - o número de pedidos realizados; II - a listagem dos provedores de conexão ou de acesso a aplicações aos quais os dados foram requeridos; III - o número de pedidos deferidos e indeferidos pelos provedores de conexão e de acesso a aplicações; e IV - o número de usuários afetados por tais solicitações.

[145] Para saber mais, acessar: <https://faq.whatsapp.com/pt_br/android/28030015/>. Acesso em: 11 set. 2017.

[146] I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[147] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Elencando a ANATEL, a Secretaria Nacional do Consumidor (Senacon) e o Sistema Brasileiro de Defesa da Concorrência (SBDC) como entes aptos à fiscalização nos termos de suas disposições, fazendo menção, ainda, ao Comitê Gestor da Internet (CGI.br), o decreto foi impreciso na distribuição das competências regulatórias, demandando esforço interpretativo e em conjunto com outros diplomas legais para a retirada de algum sentido da norma.

De toda forma, e pelo até aqui exposto, é possível perceber que, das entidades elencadas, somente a Senacon, pelas disposições do CDC, oferecem certa guarida ao consumidor no que tange à proteção dos dados pessoais, principalmente em relação à informações claras sobre termos de uso e licenças (com destaque às cláusulas que impliquem em limitação de direito, como as que exploram a privacidade do usuário), ao livre acesso aos próprios dados e à possibilidade de correção dos mesmos. O CGI.br, vale ressaltar, é órgão de caráter técnico-orientador, não possuindo as características conformadoras de um ente regulatório[148]. Este assunto será abordado em maior detalhe no capítulo quatro.

2.4.4 Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), oriunda do Projeto de Lei da Câmara nº 53/2018, por sua vez um substitutivo a outros dois projetos de lei (PL 4060/2012 e 5276/2016)[149], sancionada no dia 14 de agosto de 2018, merece atenção por duas razões: primeiro, como já dito, porque congrega disposições de projetos de lei que também contaram com processos amplos de conformação, recebendo contribuições de vários setores da sociedade[150] e ostentando, em razão disto, disposições modernas e em consonância com diplomas de mesma natureza de outros

[148] A Portaria Interministerial n° 147, de 31 de maio de 1995, criou o referido órgão; foi complementado em 2003 pelo Decreto nº 4.829, que dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.br, sobre o modelo de governança da Internet no Brasil, e dá outras providências. Da análise do art. 1º do seu Decreto criador, que estabelece suas atribuições, infere-se que o CGI.br não possui independência e autonomia, pois que composto de membros advindos do meio empresarial; não tem poderes de conciliação, sendo incapaz de mediar conflitos existentes tanto entre consumidores e empresas reguladas, ou mesmo entre entes regulados e o governo; e carece de poderes fiscalizatório e sancionatório, sendo incapaz de impor coercitivamente suas normativas e orientações.

[149] "A chamada Lei Geral de Proteção de Dados Pessoais é o PLC (Projeto de Lei da Câmara) 53/2018, resultado da união de outros dois projetos mais antigos que caminhavam juntos na Câmara – o PL 4060/2012 e o 5276/2016". RONCOLATO, Murilo. **O que diz o projeto de lei de proteção de dados que tramita no Senado**. Disponível em: <https://www.nexojornal.com.br/expresso/2018/06/07/O-que-diz-o-projeto-de-lei-de-prote%C3%A7%C3%A3o-de-dados-que-tramita-no-Senado>. Acesso em: 08 jul. 2018.

[150] "[…] o texto do PL 5276/16 ganha destaque entre os demais projetos de lei em tramitação. Esta opção se deve às seguintes considerações: i. O PL 5276/16 traz maior embasamento em regras e conceitos relacionados à coleta e tratamento de dados; ii. Das três proposições legislativas, este projeto é o que mais foi submetido à discussão pública e a debates democráticos, mediante participação de diferentes setores da sociedade civil em sua redação e por repetidas consultas públicas; iii. O projeto pondera de forma mais específica e mais completa acerca da criação de uma autoridade encarregada da fiscalização, aplicação e complementação normativa da futura lei - algo essencial, na visão deste relatório, para atingir seus objetivos de modo mais eficaz". SILVA, Alexandre Pacheco da (Coord.). **Um novo mundo de dados**: relatório final. São Paulo: FGV, 2017. p. 12

países[151]; segundo, porque é a lei, por excelência, reguladora e normatizadora das situações que envolvem dados pessoais, tanto pela iniciativa privada como pelo Poder Público. Desta forma, mantendo íntima relação com o objeto do trabalho, faz-se breve esforço analítico sobre este diploma legal.

A Lei Geral de Proteção de Dados Pessoais "dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014", o Marco Civil da Internet. Vem, desta maneira, suprir a lacuna deixada pelo legislador quanto ao teor do art. 3º, III, deste diploma. A LGPD sofreu, conforme já mencionado, muitos vetos e algumas modificações por parte da Presidência

Seu artigo primeiro expressa o alcance da LGPD, que disporá sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de *proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural*. Grifamos a última parte desta pela concordância que ostenta o dispositivo com as ideias previamente adotadas pelo trabalho acerca da privacidade, seu conteúdo e a proteção de dados pessoais.

O direito fundamental à liberdade toma papel de protagonismo ao lado da privacidade, coadunando-se com os argumentos até então elencados; ao mesmo tempo, o legislador, sem receio de parecer redundante, deixa expressa como também protegida a liberdade de desenvolvimento da personalidade da pessoa natural, construindo assim um diploma capaz de abarcar os diferentes aspectos da privacidade e dos valores a ela conexos, precavendo-se ante a complexidade da situação em que os dados pessoais estão inseridos.

O art. 2º, por sua vez, elenca sete fundamentos à disciplina da proteção de dados pessoais. São eles: 1) o respeito à privacidade; 2) a autodeterminação informativa; 3) a liberdade de expressão, de informação, de comunicação e de opinião; 4) a inviolabilidade da intimidade, da honra e da imagem; 5) o desenvolvimento econômico e tecnológico e a inovação; 6) a livre iniciativa, a livre concorrência e a defesa do consumidor; e 7) os direitos humanos e o livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoais naturais.

São fundamentos que continuam em linha com as ideias expostas e defendidas pelos estudiosos do tema no país; atuando como delineações gerais, como balizas e limites, estes fundamentos conseguem englobar a complexidade que a contextualização da privacidade no âmbito da proteção de dados pessoais ostenta, tal qual demanda, também, a analogia com a metáfora de luz e sombra. Fundamentos que logram encaixar não apenas o respeito à privacidade, aos direitos humanos, à liberdade e valores conexos à dignidade da pessoa humana na regulamentação do

[151] Por exemplo, a definição de dados pessoais: "A definição do PL 5276/16 também está de acordo com o Article 4, (1) da Regulation (EU) 2016/679, lei geral de proteção de dados editada pelo Parlamento Europeu e pelo Conselho Europeu". SILVA, 2017, op. cit., p. 86

tratamento de dados pessoais, mas também o desenvolvimento econômico, tecnológico, a inovação, a livre iniciativa e livre concorrência.

É dizer, a proteção dos dados pessoais, ao mesmo passo que intenta proteger a privacidade dos sujeitos de direito, igualmente alcança a construção de um cenário que não engessa, amordaça ou interrompe o desenvolvimento econômico, tecnológico e, igualmente, as vontades e interesses envolvidos. Neste azo, estariam englobadas diversas situações que já são vivenciadas no paradigma da sociedade em rede, como, por exemplo, a superexposição voluntária de certos sujeitos nas redes sociais virtuais; abrindo mão de parcela significativa de sua privacidade e liberdades, algumas pessoas fazem da exposição em redes sociais como *Facebook, YouTube* e *Instagram* um meio de vida, voluntariamente mitigando o conteúdo da sua sombra tutelada pela privacidade.

Seu art. 3º expressa termos similares aos já previstos no art. 11º do Marco Civil da Internet, estipulando que a lei aprovada aplicar-se-á a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que observadas determinadas condições[152].

Por sua vez, o art. 4º estipula situações de exceção à aplicação da eventual Lei Geral de Proteção de Dados Pessoais, como aquelas hipóteses de tratamento por pessoa natural para fins exclusivamente particulares e não econômicos, aqueles com finalidade jornalística, artística ou acadêmica, tratamento com fins exclusivos de segurança pública, defesa nacional, segurança de Estado ou de atividades de investigação e de repressão de infrações penais, entre outras[153].

Destaque merece o parágrafo 2º deste dispositivo, que expressamente veda o tratamento de dados, por pessoa de direito privado, com fins de segurança pública, defesa nacional, segurança de Estado ou de atividades de investigação e de repressão de infrações penais, reverberando uma vez mais a cautela do legislador em proteger a privacidade, a liberdade e a dignidade dos sujeitos de direito.

---

[152] I – a operação de tratamento seja realizada no território nacional; II – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso III do caput do art. 4º desta Lei.

[153] IV – provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

O art. 5º tratou de trazer as denominações utilizadas pela LGPD: além de definir o que é dado pessoal (informação relacionada à pessoa natural identificada ou identificável), traz ainda a definição de dados sensíveis[154] e dados anonimizados[155].

A especificação de dados sensíveis é de suma importância na conformação da proteção à privacidade, já que são dados relacionados a questões que, em possível violação da privacidade, podem ter consequências nefastas – a exemplo do já aludido caso da minoria étnica dos *rohingya* em Myanmar. Conferir maior proteção a estes dados, que relacionam-se intrinsecamente à liberdade, dignidade e livre desenvolvimento da personalidade é imprimir maior força à tutela da privacidade e seus valores atrelados. É de se entender, ainda, como sendo os dados pessoais sensíveis como espécie do gênero dado pessoal, apenas demandando maior cuidado em sua proteção e cuidado.

Por outro lado, a anonimização é, apesar das críticas[156], ainda uma ferramenta necessária para, senão impedir, ao menos coibir e dificultar eventuais violações à privacidade: desidentificar os dados, atribuindo codinomes, códigos ou outros elementos distintivos referentes aos titulares dos

---

[154] "II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".
Para Alexandre Pacheco da Silva, "A delimitação [deste] conceito é fundamental para o resguardo de direitos fundamentais em um contexto democrático, na medida em que a divulgação ou utilização inconsequente de dados sensíveis pode gerar uma exposição indevida de seu titular. Nesse sentido, por exemplo, dados pessoais de pacientes médicos trazem profundas implicações éticas sobre engenharia genética, controle populacional, discriminação baseada em predisposição a doenças e até eugenia. A definição precisa e adequada do termo também é condição para a segurança jurídica, uma vez que informaria aos atores regras claras sobre os procedimentos a serem seguidos no tratamento desses dados e nas limitações a serem observadas". SILVA, op. cit., p. 86

[155] "III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".
Sobre a anonimização, Alexandre Pacheco da Silva afirma que "Trata-se de elemento frequentemente tido como essencial à garantia do direito à privacidade, uma vez que obriga o tratamento de dados de modo que ele não guarde mais referências individualizadas a nenhuma pessoa natural em específico. No entanto, a própria possibilidade de anonimização total e irreversível de dados pessoais é tecnicamente questionável, uma vez que a emergência de novas técnicas de engenharia reversa pode reverter esse tipo de tratamento, possibilitando a identificação de indivíduos específicos. Nesse sentido, mesmo anonimizados, tais dados continuariam a ser pessoais, pois ainda seriam referentes a pessoas identificáveis". Ibidem, p. 87

[156] As críticas revolvem sobretudo ante a frágil capacidade de os conjuntos de dados anonimizados permanecerem anônimos. Existem variadas técnicas que podem ser utilizadas na reidentificação de tais dados: "In 2000, Sweeney showed that 87 % of the U.S. population can be uniquely reidentified based on five-digit ZIP code, gender, and date of birth. Datasets released prior to that publication and containing such data became subject to reidentification through simple cross-referencing with voter list information. For example, through comparison with the Social Security Death Index, an undergraduate class project re-identified 35 % of Chicago homicide victims in a de-identified dataset of murders between 1965 and 1995. Furthermore, because research findings do not get put into practice immediately, datasets still are being released with this type of information: Sweeney showed that demographic information could be used to re-identify 43 % of the 2011 medical records included in data sold by the state of Washington, and Sweeney, Abu, and Winn demonstrated in 2013 that such demographic cross-referencing also could re-identify over 20 % of the participants in the Personal Genome Project, attaching their names to their medical and genomic information". NARAYANAN, Arvind; HUEY, Joanna; FELTEN, Edward J. A Precautionary Approach to Big Data Privacy. pp. 357-386 In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (ed.). **Data Protection on the Move**: Current Developments in ICT and Privacy/Data Protection. Law, Governance and Technology Series, Issues in Privacy and Data Protection, vol. 24. Dordrecht: Springer, 2015. p. 361

dados ainda se faz necessário como uma camada protetiva, uma etapa de dificuldade imposta à eventuais e potenciais violações – uma espécie de "cadeado no portão", assim como a utilização de criptografia e outras tecnologias promotoras de privacidade (PET, na sigla em inglês)[157].

Destacamos ainda, deste dispositivo, as definições de titular[158]; controlador, operador e encarregado[159]; tratamento[160]; anonimização[161]; consentimento[162]; e relatório de impacto à proteção de dados pessoais[163]. No prisma a ser adotado no capítulo quatro, são conceitos que terão importância na consecução da perspectiva de regulação. Em síntese, são elementos conceituados que conferem, em conjunto, maior segurança jurídica nas relações envolvendo dados pessoais, maior proteção a estes dados e conferem mais força aos direitos e prerrogativas dos titulares dos dados. Serão tratados com maior ênfase no referido capítulo.

Buscando ainda orientar o tratamento de dados pessoais, o art. 6º do PLC 53/2018 estipula princípios a serem observados nestas atividades. Dentre eles, o princípio da boa-fé, previsto no *caput*, e os princípios da *finalidade* (realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades), da *adequação* (compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento), da *necessidade* (limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados), *livre acesso* (garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais), *qualidade dos dados* (garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento), *transparência* (garantia, aos titulares, de

[157] "Privacy enhancing technologies (PETs) that guarantee some type of data confidentiality and hence user privacy have been an important research topic ever since. The data that is kept confidential using PETs may be stored data, communicated data, or the conditions of a given communication — most often limited to the anonymity of the sender and/or receiver of the communication". GÜRSES, Seda; BERENDT, Bettina. **PETs in the Surveillance Society**: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm. In: GUTWIRTH; POULLET; DE HERT (ed.), op. cit., p. 302

[158] V – titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

[159] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;

[160] X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

[161] XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

[162] XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

[163] XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial), *segurança* (utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão), *prevenção* (adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais), *não discriminação* (impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos) e *responsabilização e prestação de contas* (demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas), em seus incisos.

São princípios, como se vê, que imprimem maior força à LGPD e a possível sombra que poderá lançar na tutela dos conteúdos imbricados na privacidade. Ressalte-se que tratam-se de princípios já bastante debatidos pela doutrina nacional[164] e presentes em outros diplomas legais similares, a exemplo da GDPR europeia. Como se verá no capítulo quatro, são princípios que também se alinham aos nortes regulatórios propostos neste trabalho, levando para os aspectos técnicos da proteção dos dados pessoais e da privacidade o viés legal e jurídico, em um esforço de fortalecimento da *privacy by design* (privacidade por design).

No art. 7º, a LGPD estipula um rol de hipóteses nas quais o tratamento de dados poderá ser realizado. No inciso I, fica expressa a necessidade de consentimento pelo titular, ressaltando a proeminência do direito à autodeterminação informativa no contexto do tratamento de dados pessoais; no inciso II, consigna-se que o tratamento poderá ser realizado para o cumprimento de obrigação legal ou regulatória pelo controlador; os incisos III e IV tratam das hipóteses de tratamento pela administração pública e por órgãos de pesquisa (sendo garantida, sempre que possível, a anonimização dos dados pessoais); o inciso V prevê a possibilidade em caso de execução de contrato ou de procedimentos preliminares relacionados a contrato do qual é parte o titular, a pedido do titular dos dados; o inciso VI afirma a possibilidade no exercício regular de direitos em processo judicial, administrativo ou arbitral; inciso VII, para a proteção da vida ou incolumidade física do titular ou de terceiro; VIII, para a tutela da saúde; inciso IX, para atender aos interesses do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; e, finalmente, o inciso X, para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

[164] Danilo Doneda, por exemplo, já fazia menção, em 2006, a alguns dos princípios indicados acima, dentre eles o princípio da transparência (ou publicidade), da qualidade dos dados (ou da exatidão), da finalidade, do livre acesso e da segurança física e lógica. O autor considera este rol de princípios como sendo um "núcleo comum" de várias normativas sobre proteção de dados pessoais. De maneira semelhante, já em 2008, Laura Schertel Mendes também aborda uma série de princípios para a proteção de dados pessoais, mencionando o princípio da publicidade (transparência), da exatidão, finalidade, livre acesso e segurança. Cf.: DONEDA, op. cit., 2006, p. 215-217; e MENDES, op. cit., 2008, p. 56-57.

Como se pode inferir a partir de uma ligeira análise dos termos supra, o legislador elaborou extenso rol de hipóteses nas quais o tratamento de dados pessoais é possível – ressalte-se que a presença do termo "somente", no caput, deixa a interpretação de que é um rol exaustivo e não extensivo. Apesar disto, são hipóteses aparentemente bem compreensivas, e que prezam não só pela proteção dos direitos dos titulares, mas também de outros interessados, a exemplo do inciso X.

Imperioso destacar o teor do § 6º do dispositivo *sub examine*, que afirma que eventual dispensa da exigência do consentimento do titular não desobrigará os agentes do tratamento das demais obrigações previstas pela LGPD, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Resta clara mais uma vez, aqui, a intenção do legislador com a proteção dos direitos do titular dos dados pessoais, eliminando a ausência de consentimento como causa ensejadora de utilização desregrada dos dados pessoais; bastante louvável é esta postura, sobretudo em razão das acertadas críticas formuladas por estudiosos[165] do tema, que apontam a falibilidade do sistema de *notice and consent* (informação e consentimento, em tradução livre) na coleta e tratamento de dados pessoais: é falho tanto[166] pelo aspecto de vulnerabilidade entre titular e agente de tratamento, sem ter o titular o real alcance de como se dá a coleta e tratamento, como pelo aspecto da transmissão de dados – é possível que o titular tenha consentido para um agente que, por sua vez, negociou os dados pessoais com um terceiro, para o qual o titular jamais consentiu.

O art. 8º, em esforço para superar estas questões, estabelece previsões como a do § 1º, que determina que a cláusula do consentimento seja destacada das demais cláusulas contratuais, do § 3º, que veda o tratamento de dados pessoais mediante vício de consentimento, e o esclarecimento quanto a finalidade do tratamento para informação do consentimento, no § 4º.

De forte importância para o trabalho é o teor dos arts. 11 a 13, que abordam o tratamento dos dados sensíveis.

---

[165] "In the case of consent, too, commonly perceived operational challenges have distracted from the ultimate inefficacy of consent as a matter of individual choice and the absurdity of believing that notice and consent can fully specify the terms of interaction between data collector and data subject". BAROCAS; NISSENBAUM, op. cit., p. 45

"When people give consent, they must often consent to a total surrender of control over their information. Collection of information is often done by misleading the consumer". SOLOVE, 2004, op. cit., p. 51

"Outro fator é que o consentimento para o tratamento de dados pessoais aparenta ser um procedimento inócuo, dado que os seus efeitos não demonstram contornos muito nítidos ao interessado – é nítida a extrema facilidade de mascarar os reais efeitos deste tratamento, tornando-os difíceis de serem identificados ou mesmo invisíveis". DONEDA, op. cit., 2006, p. 373-374

[166] "The reasons why a priori controls lose effectiveness are varied: first, more and more data is collected without the subject knowing it (through various logs, web cookies, surveillance systems, mobile phone applications leaking personal data to application providers or third parties, etc.). Even when the subject is aware of the data collection and asked to provide his consent, this consent has become a fictitious protection because he generally does not take the time to read the privacy notice provided by the controller, does not understand its implications, or gives his consent for lack of a real alternative (because he needs to get access to information or to a service)". BUTIN, Denis; CHICOTE, Marcos; LE MÉTAYER, Daniel. **Strong Accountability**: Beyond Vague Promises. In: GUTWIRTH, Serge, et al (eds.), 2014, op. cit., pp. 343-369. p. 352

O art. 11 estipula as previsões de permissibilidade do tratamento de dados sensíveis, o art. 12 equipara os dados anonimizados aos dados pessoais quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido, ao passo que o art. 13 trata dos casos em que se utilizem os dados sensíveis na realização de estudos em saúde pública.

Mister ressaltar o art. 12, quanto à crítica à anonimização como solução à proteção de dados pessoais: há autores[167] que apontam os perigos da anonimização (ou "desidentificação") de dados, demonstrando exemplos de como é possível[168] fazer o "caminho inverso" e encontrar, com relativa facilidade, os titulares dos dados sensíveis ou pessoais.

Necessário mencionar o teor do art. 14, que dedicou-se a tutelar o tratamento dos dados pessoais de crianças e de adolescentes. Dispõe que este tratamento deverá ser realizado no melhor interesse dos menores, nos termos deste artigo e da legislação pertinente – desta forma ensejando que o tratamento deve respeito igualmente ao Estatuto da Criança e do Adolescente.

Seu parágrafo primeiro determina a necessidade de consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal para que haja o tratamento destes titulares. O parágrafo terceiro, por sua vez, estipula uma exceção à regra do primeiro, quando a coleta for necessária para contatar os pais ou responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento previsto no parágrafo primeiro.

O parágrafo quarto é de extrema pertinência, ainda mais por direcionar a tutela em um nicho que congrega com maior intensidade crianças e adolescentes: o dos jogos e aplicações de internet correlatas. Este dispositivo prevê que os controladores não deverão condicionar a participação dos titulares ao fornecimento de informações pessoais além das estritamente necessárias à atividade, de forma que não sejam os jovens demasiadamente explorados.

Mencionar os arts. 15 e 16, que tratam do término do tratamento, também é necessário, já que preveem os marcos que imporão o encerramento do tratamento dos dados pessoais.

---

[167] Sobre um estudo feito com a Netflix e dados anonimizados, Adam Tanner explica que pessoas foram capazes de reidentificar pessoas, mesmo a partir de dados anonimizados: "As a further check, they reidentified two colleagues who had shared their Netflix viewing data with them, so in those two cases they knew for sure that their method worked and that they had found the right people. The findings illustrated the privacy dangers that massive amounts of personal data pose, even if stripped of names". TANNER, op. cit., p. 111

Ainda sobre o tema, Barocas e Nissenbaum: "In practice, however, anonymity and consent have proven elusive, as time and again critics have revealed fundamental problems in implementing both". Op. cit., p. 45

[168] "The same kinds of techniques that reveal intimate information from Facebook can help outsiders figure out who you are when you have not identified yourself. The vast proliferation of personal data as well as advances in computing power have made it harder to maintain anonymity. That's because some parts of a person's data could match with another dataset about them with more identifying details. It is as if several city maps had been ripped into pieces. An individual piece might not show enough to recognize the place, but a few pieces together would". Ibidem, p. 101-102

Assim, são hipóteses que importam no encerramento, conforme o art. 15, a verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; o alcance do fim do período de tratamento; a comunicação do titular, inclusive no exercício do seu direito de revogação do consentimento conforme disposto no § 5º do art. 8 da lei, resguardado o interesse público; ou por determinação da autoridade nacional, quando houver violação do disposto nesta lei.

O art. 16, por sua vez, afirma que os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizando a conservação dos mesmos para quatro hipóteses: para o cumprimento de obrigação legal ou regulatória pelo controlador; em razão de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; face a transferência a terceiros, desde que respeitados os requisitos de tratamento de dados dispostos na lei; ou pelo uso exclusivo do controlador, vedado o seu acesso por terceiros, e desde que anonimizados os dados.

Os arts. 17 a 22 tratam dos direitos do titular e, portanto, merecem destaque. O caput do art. 17 é expresso em garantir os direitos à liberdade, intimidade e privacidade a toda pessoa natural, assim como o direito à titularidade de seus dados pessoais. Como se vê, constata-se uma vez mais a preocupação do legislador em salvaguardar a privacidade e a liberdade, de forma que as ideias até aqui defendidas encontram ressonância na legislação nacional.

O art. 18 elenca um rol de direitos passíveis de exigência por parte do titular em face do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: direito à confirmação da existência de tratamento; de acesso aos dados; de correção de dados incompletos, inexatos ou desatualizados; à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta lei; à portabilidade dos dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; e à eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta lei; informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

São direitos que priorizam a vontade do titular dos dados, capacitando-os de prerrogativas aptas a empoderá-los e fazer valer os seus direitos frente aos controladores – controladores estes que, não raro, são empresas gigantes como o *Google* ou o *Facebook*.

O capítulo IV versa sobre o tratamento de dados pessoais pelo poder público e, portanto, suas disposições são prescindíveis ante o objeto de estudo do presente trabalho.

Por seu turno, o capítulo V traz disposições acerca da transferência internacional de dados. O art. 33 elenca as hipóteses de permissão[169], e os arts. 34 a 36 tratam de aspectos procedimentais dos acordos entabulados quanto à transferência de dados. Estipulam certas prerrogativas à autoridade nacional de proteção de dados, que poderá designar organismos de certificação para as atividades de que tratam. São inegáveis esforços em salvaguardar os direitos dos titulares dos dados, procurando alternativas diante do cenário de fragilidade de aplicação das normas nacionais diante de uma sociedade em rede.

Do art. 37 ao 45, a LGPD discorre sobre os agentes de tratamento de dados pessoais – o controlador, o operador e o encarregado, assim como das possibilidades de responsabilidade e do ressarcimento de danos. Extremamente oportunas essas previsões, uma vez que retiram da generalidade de uma empresa ou companhia a responsabilidade em casos de violação, destrato ou negligência no manuseio dos dados, apontando responsáveis, pessoas a quem dirigir, eventualmente, pleitos reparatórios170.

Do art. 46 ao art. 54, o legislador tratou de discorrer sobre a segurança e sigilo de dados, estabelecendo parâmetros, medidas e procedimentos para tanto; das boas práticas e da governança em termos de tratamento de dados pessoais, ensejando a possibilidade de autorregulação, pacificação de *standards* (padrões), entre outras formas de consenso e regramento entre os agentes; da fiscalização, prevendo a possibilidade de sanções administrativas a serem aplicadas face o cometimento de infrações – infrações estas a serem estipuladas, fiscalizadas e com sanções a serem impostas pelo órgão competente.

O órgão competente de que a LGPD menciona se vê no art. 55, que foi vetado juntamente com os artigos 56 a 59 e que compreendiam as Seções I e II do Capítulo IX: tratava-se da

[169] I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos; III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; V - quando a autoridade nacional autorizar a transferência; VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei. Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Autoridade Nacional de Proteção de Dados (ANPD), órgão integrante da administração pública federal indireta, submetido a regime autárquico especial e vinculado ao Ministério da Justiça, que deverá ser regida segundo os termos da lei no 9.986, de 18 de julho de 2000 (lei das agências reguladoras).

A LGPD previa ainda a criação do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, entidade de caráter multiparticipativo, comporto por 23 (vinte e três) representantes titulares advindos do Poder Executivo Federal, indicados pelo Senado e pela Câmara, indicados pelo Conselho Nacional de Justiça e Conselho Nacional do Ministério Público, representante do Comitê Gestor da Internet no Brasil (CGI.br), representantes da sociedade civil com expertise em proteção de dados pessoais, representantes de instituições científicas, tecnológicas e de inovação e representantes do setor empresarial afeto à área de tratamento de dados pessoais.

A este órgão competirá propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e de atuação da Autoridade Nacional de Proteção de Dados, elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade, sugerir ações a serem realizadas pela ANPD, realizar estudos e debates sobre a proteção de dados pessoais e da privacidade e disseminar o conhecimento sobre proteção de dados pessoais e da privacidade à população.

Aqui há que se abrir parêntese para externar certo descontentamento, generalizado[170] entre a comunidade acadêmica especializada, com o veto da presidência quanto à criação da ANPD. Esta Autoridade, concebida nos moldes das agências reguladoras nacionais, centralizaria a regulação do tratamento de dados pessoais no país. A sua não criação enfraquece sobremaneira a fiscalização e aplicação dos ditames da LGPD, fragmentando a competência para regular em diversos entes, como se verá no capítulo quatro.

Todavia, e como se pode ver, é uma lei bastante compreensiva, posto que baseada em projetos de leis bem trabalhados[171], e logra discorrer sobre muitos dos aspectos levantados em

---

[170] "O resultado é a aprovação de uma lei que cria pesadas obrigações jurídicas, mas é acéfala. Em outras palavras, é uma lei morta-viva. Tal como um zumbi de seriado de televisão, suas normas serão colocadas em movimento." LEMOS, Ronaldo. **Lei de dados nasceu desgovernada**. Disponível em: <https://www1.folha.uol.com.br/colunas/ronaldolemos/2018/08/lei-de-dados-nasceu-desgovernada.shtml>. Acesso em: 22 ago. 2018.
"Especialistas, no entanto, defendem que o órgão é indispensável para a aplicação das regras. Segundo Carlos Affonso de Souza, diretor do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-Rio), a lei perde força sem a agência reguladora. 'A ANPD teria o papel importante de centralizar a aplicação, evitar a pulverização de fiscalização e propor orientações de interpretação.'" LIMA, Mariana. **Lei de Proteção de Dados brasileira é criada sem agência reguladora**. Disponível em: <https://link.estadao.com.br/noticias/cultura-digital,temer-sanciona-lei-de-protecao-de-dados-mas-veta-autoridade-regulatoria,70002451106>. Acesso em: 22 ago. 2018.

[171] "Os projetos de leis gerais em tramitação no Congresso Nacional para proteção de dados pessoais —nomeadamente PL 5276/2016, PLS 330/2013 e PL 4060/2012 — oferecem diferentes garantias ao direito à privacidade". ARTIGO 19. **Proteção de dados pessoais no Brasil**: Análise dos projetos de lei em tramitação no Congresso Nacional. Coord.: Laura Tresca. São Paulo: Artigo 19, 2016. Disponível em: <http://artigo19.org/wp-

termos de privacidade e sua proteção. Neste subtópico, preferiu-se, por opção metodológica[172], resumir as menções a pontos chaves e centrais da LGPD; a sua análise esmiuçada se mostrou desaconselhável essencialmente em virtude da sua extensão e detalhamento, que seria passível mesmo de realização de um trabalho dissertativo unicamente com este desiderato.

Assim, e considerando que foi levantado o arcabouço jurídico mínimo para ilustrar a proteção da privacidade e dos dados pessoais no Brasil, abordar-se-á, no capítulo que segue, o cenário de contextualização imprescindível ao preenchimento do conteúdo protetivo da privacidade – os pontos luminosos que, emanando os feixes de potenciais riscos à violação deste direito fundamental e seus valores conexos, eventualmente ensejarão a projeção de sombras lançadas pelos diplomas que ora se elencaram.

3 SOCIEDADE EM REDE, CIBERESPAÇO, CONVERGÊNCIA DIGITAL: O PARADIGMA DA SOCIEDADE INFORMACIONAL E O PROTAGONISMO DOS DADOS

No ano de 2017, a população mundial alcançou a impressionante cifra de 7,5 bilhões de

content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>. Acesso em: 08 jul. 2018.

[172] Por razão semelhante se preferiu não abordar a General Data Protection Regulation da União Europeia no presente trabalho. Apesar de entender que as barreiras nacionais são desconsideradas no âmbito da sociedade em rede, uma análise deste diploma legal demandaria esforço que vai muito além do objeto do trabalho (que engloba o cenário nacional de monetização de dados pessoais). Ademais, se almeja com esta dissertação para contribuir na proteção do direito fundamental à privacidade dos titulares de dados pessoais brasileiros (e dos que encontram-se em território nacional, como quer o art. 3º da nossa LGPD); os europeus, que já debatem esta problemática há muito mais tempo, já estão, por conseguinte, melhor tutelados neste sentido.

seres humanos. No mesmo ano, o *Facebook* – popular rede social virtual – alcançou a marca de 2 bilhões de usuários mensais. São números que falam alto. É dizer, um quarto da população mundial, 25% de todo o mundo, acessa, mensalmente, uma única rede social – em um universo de inúmeras. Em outras palavras: o mundo está, cada vez mais, interconectado.

Inegável a influência que o avanço das Tecnologias da Informação e Comunicação, impulsionadas pelo "carro-chefe" internet, vem exercendo no planeta nas últimas três décadas. É uma mudança de paradigma que muitos estudiosos, entre historiadores, sociólogos, juristas e filósofos abordaram de diferentes maneiras e perspectivas. A sociedade, ante esta influência, metamorfoseia-se. Mudam as formas de se criar e consumir conteúdo, de interagir, de se comunicar e de fazer negócios.

Nesse cenário de uma sociedade inter (e hiper) conectada, gradualmente moldada e mais influenciada pela internet, uma das consequências imediatas é a produção de dados. Muitos dados. Em uma quantidade imensa. Estima-se que 2.5 Exabytes[173] de dados são produzidos diariamente[174] no âmbito da rede mundial de computadores.

São tantos dados, produzidos tão rapidamente e de tipos e origens diferentes, que se convencionou chamar esse cenário (e as soluções para sua lide, como os algoritmos, *machine learning* e *business inteligence*) de *big data*. Neste colossal espectro de dados produzidos e armazenados diariamente na internet, encontram-se os dados pessoais, que podem ser, em poucas palavras, definidos como os dados relacionados à pessoa natural identificada ou identificável.

Adaptando-se a este novo panorama de *big data*, a economia, cada vez mais voltada para a informação, passou a aproveitá-lo: coletando e tratando estes dados, tidos como insumos, novos modelos de negócio surgiram[175]. Os dados se tornaram tão valorizados que já chegaram a dizer se tratar do "novo petróleo". Sobre os dados pessoais, especificamente, está baseado um dos modelos

---

[173] 1 Exabyte equivale 1.000.000.000.000.000.000 (um quintilhão) de Bytes. Para se ter uma ideia: 2.5 Exabytes produzidos diariamente é o mesmo que 530.000.000.000.000 arquivos de música, ou 777.600 horas de (90 anos) de arquivos de vídeo em alta definição.

[174] BENNETT, Madeline. **How data analytics can revolutionise healthcare**. Disponível em: <https://www.telegraph.co.uk/business/open-economy/how-data-analytics-can-revolutionise-healthcare/>. Acesso em 13 jul. 2018.

WALL, Mathew. **Big data**: are you ready for blast-off? Disponível em: <https://www.bbc.co.uk/news/business-26383058>. Acesso em 13 jul. 2018.

JACOBSON, Ralph. **2.5 quintillion bytes of data created every day**. How does CPG & Retail manage it? Disponível em: <https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it/>. Acesso em 13 jul. 2018.

[175] "Empresas que começaram como startups (empresas nascentes de base tecnológica) no começo dos anos 2000, Google, Facebook, Twitter, Double Click, se tornaram empresas de grande porte com atuação internacional em 2015, criando modelos de negócio integralmente baseados em operações de coleta, tratamento e análise de dados dos usuários de seus serviços". SILVA, 2017, op. cit., p. 10

de negócio mais rentáveis[176] neste âmbito – a publicidade dirigida[177].

Em tempos de crise econômica, como a que experiencia o planeta desde a bolha imobiliária norte-americana de 2008, negócios baseados em dados surgem como uma atraente alternativa: é um insumo, como se viu, que se produz em escalas imensas diariamente, e cujo acesso, coleta e armazenamento torna-se mais barato quanto mais evoluem as tecnologias para tanto.

Serviços aparentemente gratuitos são, de igual maneira, atraentes para os usuários e consumidores em tempos de depressão econômica. Serviços *online* como o *Facebook, WhatsApp, Twitter, Instagram* e *YouTube*, entre vários outros que monetizam os dados pessoais, são de acesso 'gratuito'; muitos aplicativos para *smartfones* e *tablets* também o são – desde que, em troca da utilização deles, o usuário ceda seus dados pessoais.

Não à toa, tais companhias, apesar da crise, têm apresentado consistente crescimento econômico[178]. O lucro do *Facebook*, em 2016, foi de 10 bilhões de dólares. Em 2017, a receita do *Google* foi de 24,75 bilhões de dólares. Parece haver, portanto, via alternativa e extremamente interessante para contornar uma conjuntura de crise e criar modelos de negócio.

Há, contudo, e conforme se aludiu ao longo do trabalho, que se fazer importante ressalva quanto à monetização de dados pessoais: a preocupação à violação da privacidade dos usuários.

Tal apreensão frente a possibilidade de práticas como o *profiling* (criação de perfis de indivíduos ou grupos[179] de indivíduos a partir de determinado marcador, como o étnico, cultural,

[176] "No ano de 2011, por exemplo, segundo levantamento realizado pela Statista, as receitas advindas de operações de tratamento e análise de grandes volumes de dados por provedores de serviços na Internet totalizaram o montante de U$ 7.6 bilhões no mundo. Quatro anos mais tarde, em 2015, este valor alcançou a cifra de 22.6 bilhões de Dólares, um crescimento de cerca de 300%. Para 2017, a projeção é que o mercado de dados cresça pouco menos de 34 bilhões de Dólares em receita". Ibidem, p. 10

[177] "Além disso, os hábitos de navegação e interação dos usuários, por exemplo, são utilizados pelas grandes empresas de publicidade online – como o Google e o Facebook – para direcionar anúncios 'relevantes'. Atualmente, grande parte da vida real (lazer, trabalho, educação) dialoga com elementos do ambiente virtual – basta imaginar, por exemplo, sobre a impossibilidade de fazer uma viagem ao exterior sem uma consulta no Google ou Bing. O uso de redes sociais aumenta, ainda mais, esse vínculo entre 'real' e 'virtual'". MENEZES NETO, op. cit., p. 78

[178] "O fato de a informação ser monetizada faz com que a coleta, processamento e troca de dados sejam um negócio incrivelmente lucrativo para a iniciativa privada – o Facebook, por exemplo, fechou o ano de 2015 com faturamento de 17.92 bilhões de dólares". Ibidem. p. 152

[179] "O valor das informações obtidas não reside apenas na capacidade de armazenamento de grande volume de dados, mas, principalmente, na possibilidade de se obterem novos elementos informativos a respeito dos cidadãos a partir do tratamento desses dados. Exemplo disso é a técnica de construção de perfis pessoais em função dos quais podem ser tomadas importantes decisões a respeito dos consumidores, trabalhadores e cidadãos em geral, afetando diretamente a vida das pessoas e influenciando o seu acesso a oportunidades sociais". MENDES, op. cit., p. 24-25

"O segundo contexto jurisprudencial, em que os deveres em pauta foram tratados, é o relativo ao desenvolvimento tecnológico que cria perigos muitas vezes desconhecidos e riscos frequentemente incontroláveis para uma série de direitos fundamentais. Como exemplos, citem-se o desenvolvimento da energia atômica, da tecnologia eletromagnética, a poluição ambiental em suas várias formas, o desenvolvimento da informática que, ao permitir a criação de perfis de personalidade, ameaça o direito à privacidade, podendo criar aquilo que é conhecido na Alemanha sob a expressão der gläserne Mensch ('o ser humano de vidro')". DIMOULIS, Dimitri. MARTINS, Leonardo. **Teoria Geral dos Direitos Fundamentais**. 5ª ed. São Paulo: Atlas, 2014. p. 122

"Do policiamento preditivo até soluções para o sistema de saúde, a dinâmica é necessariamente a de agregação dos dados dos cidadãos para segmentá-los em grupos.Esse é um passo importante a ser dado para se pensar proteção de dados pessoais, não somente como um direito individual, mas, também, transindividual". MENEZES NETO, op. cit., p.

religioso, de gênero, etc) e da *surveillance*[180] (com uma vigilância cada vez mais abrangente – frequentemente justificada em nome da segurança nacional e combate ao terrorismo) não são de todo infundadas, como pôde atestar o *whistleblower* (denunciante) da NSA (Agência Nacional de Segurança dos EUA) Edward Snowden[181] – exemplo radical de que se faz, sim, necessária esta ressalva e cuidadosa atenção com o uso e coleta dos dados pessoais.

Neste cenário, torna-se cada vez mais raro, atualmente, não possuir perfis em diversos tipos de serviços *online*, principalmente quando se fala em redes sociais virtuais[182].

Este cenário encontra fundamento, por exemplo, no paradigma da sociedade em rede visionado por Manuel Castells. Para este autor, a sociedade, impulsionada por uma revolução das tecnologias da informação, muda suas bases materiais, tornando-se cada vez mais descentralizada, interconectada e interdependente[183], produzindo e reproduzindo informação em grandes quantidades. A informação passa a ter papel central[184] nesta sociedade, principalmente na economia[185], podendo por isso ser chamada também de sociedade informacional.

Para ele, "as redes" são formadas por nós[186](como pontos de amarração em uma rede de pesca); nós sendo a representação das confluências e influxos de poderes e vontades; são exemplos de nós os interesses econômicos, comerciais, as influências sociais e políticas, os agentes estatais de

---

57

[180] "Logo, o referido autor também concorda com a ideia de que o problema real da surveillance no mundo contemporâneo envolve, especialmente, a coleta de dados por parte da iniciativa privada. Ou seja, ao invés de ser a ferramenta de um Big Brother opressor, a surveillance é utilizada por uma infinidade de "little sisters", cujo objetivo principal é conhecer melhor o indivíduo-consumidor através da invasão de todas as esferas da sua vida. A surveillance deixa de ser uma característica de um Estado burocrático vigilante e passa a ser um traço da sociedade contemporânea". Ibidem, p. 117

[181] "A desnacionalização e a desestatização da informação colocam em cheque o ideal de soberania indivisível. Isso não implica, contudo, a impossibilidade de que determinados Estados tenham acesso ao fluxo mundial de informações, como ficou bem claro em virtude das recentes declarações do analista da NSA, Edward Snowden". Ibidem, p. 69

[182] Andrew Peter Sparrow afirma que, apesar de variarem em tipo, redes sociais virtuais apresentam certas características em comum, como a criação de um perfil pessoal e a possibilidade de se conectar com outras pessoas, grupos, compartilhando conteúdo. Para Tim Wu, as redes sociais lograram efetivar uma teia de conexões, embaladas pelo "efeito rede" – na qual uma rede se torna mais valorizada e poderosa quanto mais pessoas delas fizerem parte. Cf.: SPARROW, Andrew. **The law of virtual worlds and Internet social networks**. Gower: Farnham, 2012. p. 5; e WU, Tim. **Impérios da comunicação**: do telefone à internet, da AT&T ao Google. Trad. Cláudio Carina. Zahar: Rio de Janeiro, 2012. Edição em versão eletrônica (epub). Não paginado.

[183] "uma revolução tecnológica concentrada nas tecnologias da informação começou a remodelar a base material da sociedade em ritmo acelerado. Economias por todo o mundo passaram a manter interdependência global, apresentando uma nova forma de relação entre a economia, o Estado e a sociedade em um sistema de geometria variável". CASTELLS, op. cit., p. 39

[184] "o cerne da transformação que estamos vivendo na revolução atual refere-se às tecnologias da informação, processamento e comunicação. A tecnologia é para esta revolução o que as novas fontes de energia foram para as revoluções industriais sucessivas, do motor a vapor à eletricidade, aos combustíveis fósseis e até mesmo à energia nuclear" Ibidem, p. 68

[185] "Uma nova economia surgiu em escala global no último quartel do século XX. Chamo-a de informacional, global e em rede para identificar suas características fundamentais e diferenciadas e enfatizar sua interligação." Ibidem, p. 119

[186] "Rede é um conjunto de nós interconectados. Nó é o ponto no qual uma curva se entrecorta. Concretamente, o que um nó é depende do tipo de redes concretas de que falamos […] Redes são estruturas abertas capazes de expandir de forma ilimitada, integrando novos nós desde que consigam comunicar-se dentro da rede, ou seja, desde que compartilhem os mesmo códigos de comunicação." Ibidem, p. 566

poder, entre outros. A "rede das redes"[187] seria a internet, por permitir a junção dos diversos nós em escalas de tempo instantâneas, superando limites espaciais e geográficos, eliminando também a distinção entre centros e periferias[188]. Castells ainda deixa claro que a sociedade surgida neste paradigma ignora certos aspectos tradicionalmente assentados, dando gênese a novos outros e modernizando os que, todavia, persistem – como é o caso de certas indústrias e modelos de negócio.

Um ponto importante para Manuel Castells é a mudança de papel do Estado[189] nesse cenário de redes. Para o autor, estas características da sociedade informacional retirariam do Estado certa autonomia e capacidade de imposição de normas e vontades; seja pela nova conformação global, descentralizada, que ignora fronteiras geográficas, culturais e temporais[190], seja pela força lograda por outros atores – principalmente os interesses econômicos. Defende Castells que o Estado, ao invés de buscar um retorno ao monopólio do poder de imposição, deveria esforçar-se em alcançar um equilíbrio conformador de uma governança global, que o integrasse aos diversos e inúmeros interesses difusos na rede. É, sem dúvida, ponto de interesse para o presente trabalho, posto que a monetização de dados, no âmbito desta economia digital[191] baseada nas redes – constructos, como

---

[187] "A internet é a espinha dorsal da comunicação global mediada por computadores (CMC): é a rede que liga a maior parte das redes" Ibidem, p. 431

[188] "As estruturas sociais que surgiram nos últimos anos – especialmente aquelas vinculadas à globalização e ao fluxo de dados e comunicações globais – remodelam a forma de organização da sociedade. Essa nova morfologia social, típica da 'Era da Informação', organiza-se na forma de redes, cuja principal característica é a extinção de centros e periferias". MENEZES NETO, op. cit., p. 65

[189] "[…] a dissolução da soberania na rede de poder é uma consequência do surgimento de novas estruturas não estatais de autoridade e poder. Agora, vulnerável aos ataques cada vez menos específicos – e, por isso mesmo, mais inevitáveis – das diversas fontes de poder do mundo contemporâneo, o Estado sofre a reformulação das suas funções, passando a agir não mais como centro, mas como "nó" de uma rede descentralizada de poder". Ibidem, p. 69

[190] "Por outro lado, o novo sistema de comunicação transforma radicalmente o espaço e o tempo, as dimensões fundamentais da vida humana. Localidades ficam despojadas de seu sentido cultural, histórico e geográfico e reintegram-se em redes funcionais ou em colagens de imagens, ocasionando um espaço de fluxos que substitui o espaço de lugares. O tempo é apagado no novo sistema de comunicação já que passado, presente e futuro podem ser programados para interagir entre si na mesma mensagem. O espaço de fluxos e o tempo intemporal são as bases principais de uma nova cultura, que transcende e inclui a diversidade dos sistemas de representação historicamente transmitidos: a cultura da virtualidade real, onde o faz-de-conta vai se tornando realidade". CASTELLS, op. cit., p. 462

[191] "Uma característica da economia digital é a sua dependência na geração, no armazenamento, no processamento e na transferência de dados, tanto internamente como entre os países. O acesso a dados e a sua análise são de importância estratégica para aumentar a competitividade dos países em todos os setores. Os formuladores de políticas públicas precisam considerar a necessidade das empresas que, por um lado, têm de coletar e analisar dados para gerar inovação e ganhar em eficiência e, por outro, precisam levar em conta as preocupações das várias partes interessadas em termos de segurança, privacidade, movimentação e propriedade dos dados. O atual sistema de proteção de dados é fragmentado, com diferentes abordagens nos âmbitos global, regional e nacional. Ademais, muitos países em desenvolvimento ainda não possuem legislação alguma para a área. Em vez de perseguir várias iniciativas diferentes, é preferível que organizações globais e regionais se juntem sob a bandeira de uma iniciativa, ou que um número menor de iniciativas seja estabelecido e compatível em âmbito internacional". FREDRIKSSON, Torbjörn. Esforços necessários para transformar o comércio eletrônico em um motor do desenvolvimento. In: BARBOSA, Alexandre (Coord.). **Pesquisa sobre o uso das tecnologias de informação e comunicação nas empresas brasileiras**: TIC empresas 2017. São Paulo: Comitê Gestor da Internet no Brasil, 2018. Disponível em: <http://www.cgi.br/media/docs/publicacoes/2/TIC_Empresas_2017_livro_eletronico.pdf>. Acesso em 10 jul. 2018. p. 37

se viu, complexos demais para serem reduzidos às fronteiras de jurisdição nacionais – apresenta desafios[192] inúmeros.

Por sua vez, Andrew Murray aborda o surgimento de uma *digital convergence* (em tradução livre, convergência digital), baseada em quatro elementos básicos e vivenciados desde o início do século XXI: primeiro, se tornou mais fácil gerar, manipular, transmitir e armazenar informação; segundo, o custo para tanto diminuiu consideravelmente; terceiro, a informação eletrônica desenvolveu valor intrínseco, próprio, fato inexistente no dado analógico; e, por último, a geração de informação extra a partir da produção, cópia e operação de sistemas informáticos, passando o valor a habitar não apenas no átomo, mas, agora, nos *bytes*[193]. Esta ideia de convergência digital apresenta características similares à ideia de sociedade informacional colocada por Castells, principalmente pelo valor que se confere aos dados e à informação.

Pierre Lévy, para caracterizar o mesmo cenário, utiliza os termos ciberespaço e cibercultura. Ao primeiro, conceitua como um novo meio de comunicação permitido pela interconexão de computadores em escala planetária; ao segundo, especifica um conjunto de técnicas materiais e intelectuais, bem como de práticas e valores que exsurgem na esteira do ciberespaço[194].

Na sua lógica, a cibercultura daria gênese ao ciberespaço, na medida em que os inúmeros dispositivos (computadores, *hardwares*, *softwares*, sensores, memórias, processadores, cartões inteligentes, terminais de bancos, robôs, motores, eletrodomésticos, automóveis, copiadoras, fax, câmeras de vídeo, telefones, rádios, televisões, etc) conformam os pontos de sustentação do ambiente virtual[195], do ciberespaço. Este autor fala, ainda, em um conjunto complexo e parcialmente indeterminado de processos de interação, baseados na informação, que se autossustentam[196]. É proposição que também dialoga com as ideias de Castells, para quem a sociedade informacional

---

[192] "Alheio às benesses promovidas pela sociedade-rede, apura-se que o ciberespaço é pródigo em situações problemáticas, as quais suscitam necessariamente a atuação do Estado. Por um lado, em caráter promocional, o Estado tende a promover a inclusão digital, bem como conferir a infraestrutura necessária para tanto; por outro, deve agir a fim de garantir o pleno exercício dos direitos dos indivíduos e coibir eventuais violações ou ameaças". BIONI, Bruno Ricardo. Ecologia: uma narrativa inteligente para a proteção de dados pessoais nas cidades inteligentes. In: BARBOSA, Alexandre (Coord.). **Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro**: TIC governo eletrônico 2017. São Paulo: Comitê Gestor da Internet no Brasil, 2018. Disponível em: <http://www.cgi.br/media/docs/publicacoes/2/TIC_eGOV_2017_livro_eletronico.pdf>. Acesso em 10 jul. 2018. p. 171

[193] MURRAY, Andrew. **Information technology law**: the law and society. New York: Oxford University Press, 2010. p. 37

[194] LÉVY, op. cit., p. 17-25

[195] Ibidem, p. 43-44

[196] Ibidem, p. 25

proporcionaria a criação de "círculos virtuosos"[197] de criação de informação, consumo e novamente produção.

Daniel J. Solove, também utilizando o termo ciberespaço, encara-o como uma nova fronteira para a coleta de dados e de informação pessoal, sendo a internet o principal suporte para tal[198]. Yuval Noah Harari, sugerindo o conceito de "dataísmo" vai mais além, afirmando que o valor de qualquer fenômeno ou entidade seria determinado unicamente por sua contribuição a esse fluxo de criação e tratamento de dados e informações, eventualmente alcançando uma situação na qual os algoritmos tomarão o lugar das próprias pessoas na tomada das decisões[199].

Independente da nomenclatura que se prefira, é nesse panorama, de uma sociedade permeada pelas Tecnologias da Informação e Comunicação, hiperconectada, produtora, consumidora e reprodutora de dados[200], que acabamos por oferecer nossos dados pessoais, gerados pelos inúmeros dispositivos interconectados à internet.

É este o cenário de coleta e uso dos dados pessoais com fins de monetização[201], onde se desenvolvem modelos de negócio; é neste cenário que se encontra a potencialidade de conformação e violação da privacidade dos titulares dos dados, onde situam-se os focos e pontos de luz da metáfora de luz e sombra; é neste cenário sem território físico, sem fronteiras geográficas, sem limites nacionais explicitamente definidos que estão os fluxos e intercâmbios de dados e informações, esta matéria-prima abundante, renovável e extremamente valorizada.

Apesar das diferentes denominações, é possível perceber que os estudiosos concordam em certos aspectos: primeiro, a intensa e crescente interconexão dos processos, fluxos e aspectos da sociedade (econômicos, sociais, políticos, etc) neste novo paradigma; a existência, por conta disto,

---

[197] "O processamento da informação é focalizado na melhoria da tecnologia do processamento da informação como fonte de produtividade, em um círculo virtuoso de interação entre as fontes de conhecimentos tecnológicos e a aplicação da tecnologia para melhorar a geração de conhecimentos e o processamento da informação: é por isso que, voltando à moda popular, chamo esse novo modo de desenvolvimento de informacional, constituído pelo surgimento de um novo paradigma tecnológico baseado na tecnologia da informação" CASTELLS, op. cit., p. 54

[198] SOLOVE, op. cit., p. 22

[199] HARARI, Yuval Noah. **Homo Deus**: uma breve história do amanhã. Trad. Paulo Geiger. São Paulo: Cia. Das Letras, 2015. Edição em versão eletrônica (epub). Não paginado.

[200] "a difusão da tecnologia amplifica seu poder de forma infinita, à medida que os usuários apropriam-se dela e a redefinem. As novas tecnologias da informação não são simplesmente ferramentas a serem aplicadas, mas processos a serem desenvolvidos. Usuários e criadores podem tornar-se a mesma coisa. Dessa forma, os usuários podem assumir o controle da tecnologia como no caso da internet. Há, por conseguinte, uma relação muito próxima entre os processos sociais de criação e manipulação de símbolos (a cultura da sociedade) e a capacidade de produzir e distribuir bens e serviços (as forças produtivas). Pela primeira vez na história, a mente humana é uma força direta de produção, não apenas um elemento decisivo no sistema produtivo". CASTELLS, op. cit., p. 69

[201] "Collection (and the subsequent storage of the data) is followed by data *analysis.* Here the database, which includes the profiles of many individuals, is analyzed in search of knowledge which might prove helpful to the relevant firms. In many instances, the analysis points to potential uses which were not apparent at the time of collection. This is especially made possible by using data mining techniques, which apply sophisticated computing algorithms to reveal hidden patterns and clusters in the data". ZARSKY, Tal. **Responding to the Inevitable Outcomes of Profiling**: Recent Lessons from Consumer Financial Markets, and Beyond. In: GUTWIRTH; POULLET; DE HERT (ed.), op. cit., 2010. p. 56

de um "ambiente" relacional virtual (sociedade em rede, sociedade informacional, ciberespaço), no qual a informação passa a ter papel central (convergência digital, dataísmo); e a modificação, em razão destas características, das relações de poder, principalmente em relação ao Estado, que passa a ser desafiado[202], perdendo certa parcela de protagonismo – seja na formulação de políticas públicas, seja na elaboração de normativas e padrões regulatórios.

Assim é que, para o trabalho, a escolha destas nomenclaturas é irrelevante, vez que apresentam elementos similares e que detalham e destacam com acuidade o panorama da sociedade interconectada. Todavia, por razões metodológicas, adota-se, daqui em diante, o conceito proposto por Manuel Castells, por entender que engloba as demais conceituações trabalhadas; isto não quer dizer que, eventualmente, não os utilizaremos (como faremos, por exemplo, com o conceito de dataísmo para auxiliar na explicitação dos perigos e riscos à privacidade e aos valores seus valores conexos).

Se preferiu a "sociedade em rede/sociedade informacional" para designar este "ambiente" no qual estão inseridas as problemáticas trabalhadas para ilustrar o cenário onde se dá a coleta, tratamento e monetização dos dados pessoais: em outras palavras, para designar o panorama no qual se desenrola a equação conformadora do conteúdo protetivo da privacidade – o local, ou locais, nos quais transitam os titulares dos dados e sujeitos de direito e onde estão os focos de luz, os objetos tutelantes, lançadores de sombra, e as sombras projetadas.

Desta forma, no próximo tópico, elencaremos alguns exemplos de como os dados pessoais são utilizados e monetizados para, então, demonstrar como surgem as preocupações com a proteção ao direito fundamental à privacidade e de outros valores advindos da dignidade da pessoa humana.

3.1 OS DADOS COMO O "NOVO PETRÓLEO": EXEMPLOS DE MODELOS DE NEGÓCIO QUE OS MONETIZAM

Como se viu, viver em sociedade, atualmente, significa em grande parte viver conectado: conectado às mais diversas redes sociais, aos serviços de *e-mail*, aos portais e *feeds* de notícias e entretenimento; é poder levar a qualquer lugar e acessar a qualquer tempo estas informações. Levamos hoje nos bolsos e na palma da mão os dispositivos que nos permitem ficar conectados e ter acesso aos vários serviços *online*.

[202] "Para dar conta deste cenário, diversos países criaram os seus modelos jurídicos de proteção dados pessoais, definindo, por exemplo: (i) seu conceito; (ii) os requisitos para operações de coleta, tratamento, análise e descarte de dados; (iii) os agentes responsáveis nestas operações; (iv) as regras para a transferência internacional dos mesmos; (v) as autoridades regulatórias da proteção de dados pessoais, dentre outros tópicos. Tais tentativas estão sendo colocadas à prova pelas constantes transformações nas atividades de tratamento de dados e pelas peculiaridades setoriais de determinados segmentos da economia". SILVA, op. cit., p. 10

Manter-se a par dos acontecimentos, informado e atualizado, torna-se de suma importância seja para a vida profissional, acadêmica, para o relacionamento com colaboradores e subordinados ou mesmo para uma melhor eficiência no dia a dia.

Assim, buscamos estar conectados, acompanhando o que acontece ao nosso redor, e para isso criamos inúmeras contas, *logins* e *perfis*, deixando uma miríade de dados e informações pela *web* em *sites* de notícias, redes sociais e lojas virtuais. Estas informações produzidas, conforme já debatido, por vezes encontram-se dentro do âmbito protetivo da privacidade, fazendo jus a um mínimo de proteção (como a numeração de cartões de crédito, de documentos, fotos e dados sensíveis, etc).

Nosso hábito de uso da internet, que tipos de sites visitamos, quanto tempo passamos em cada um deles, quais as nossas preferências quando compramos algo on-line e até mesmo a nossa localização geoespacial são também exemplos de dados e informações que geramos diariamente.

Alguns dos serviços utilizados por usuários da *web*, oferecidos por empresas[203] como o *Google, Facebook, Twitter, WhatsApp*, entre inúmeras outras, utilizam em proveito próprio os mais variados dados e informações deste "rastro digital"[204] que deixamos no ciberespaço, monetizando-os — pelo tratamento, cruzamento e análise deles ou na construção de modelos de negócio neles baseados, gerando retornos financeiros consideráveis[205].

Essa monetização se dá no âmbito da sociedade em rede, valendo-se de soluções de "*Big data*"[206] — conceito que envolve a captação, armazenamento, processamento e capitalização de

---

[203] "As empresas com as quais fazemos negócios com frequência reúnem regularmente uma quantidade enorme de informações sobre nós. […] Existem duas razões pelas quais elas armazenam um repertório sobre o consumidor. A primeira, e mais comum, é conhecer seu público-alvo, para que possam direcionar melhor as propagandas. […] A segunda razão […] é muito menos agradável: coletar nossas informações cadastrais para vender a outras empresas que têm a intenção de nos enviar propagandas. O caso mais corriqueiro dessa prática é o Facebook, para o qual fornecemos nossos dados de bom grado, sem pestanejar". CHERRY, op. cit., p. 2-3.

[204] "A empresa armazena uma enorme quantidade de dados dos usuários. Além das informações do perfil e postagens, armazena metadados como data e horário de conexão, dispositivo utilizado, endereços IPs de onde conectou, informações do navegador, cookies armazenados, 'cliques' realizados – assim como dia/hora e número de vezes, tópicos dirigidos ao usuário associado aos gostos e interesses do timeline, apps que utiliza, todas as conversas de chat realizadas, todos os likes dados, os compartilhamentos feitos, todas as fotos e vídeos postadas e seus metadados, grupos que participa ou participou, todas as pessoas que clicaram like em lugares, eventos, cidades que você logou, todas as buscas que realizou no site, os amigos que você removeu da conta e uma série de outras informações, mesmo que você já as tenha deletado (Facebook, 2015). O Facebook praticamente não apaga do que foi publicado e registra as interações feitas na plataforma da empresa, seja de forma ativa ou passiva". MACHADO, Jorge; MORETTO, Márcio. Riscos e incertezas no uso do Facebook como plataforma de ativismo político. In: THEMOTEO, Reinaldo J. (Org.). **Cadernos Adenauer XVI, nº 3**: Internet e sociedade. Rio de Janeiro: Fundação Konrad Adenauer, 2015. pp. 113-132., p. 117

[205] "This field, known as 'online behavioral advertising', is grabbing an increasingly large share of the hundreds of billions of dollars companies spend annually urging the masses to buy". Em tradução livre, "este campo [de negócios], conhecido como 'publicidade comportamental', está tomando uma crescente fatia das centenas de bilhões de dólares que as empresas gastam para fazer as massas consumirem". TANNER, op. cit., p. 157

[206] "Tais preocupações coadunam-se com a atual evolução do cenário tecnológico, em que se discute a utilização do Big Data, conjunto de soluções tecnológicas capaz de lidar com uma imensa quantidade de dados estruturados e não estruturados em volume, variedade, velocidade, variabilidade e complexidade até então inéditos. Essa ferramenta permite analisar praticamente qualquer tipo de informação digital, em tempo real, uma vez que viabiliza inclusive a compreensão de dados não estruturados que, mesmo estando em maior número na rede, antes só podiam ser

dados e informações com o intuito de auferir toda sorte de vantagens. Através do tratamento de dados, é possível aprimorar, por exemplo, a publicidade dirigida[207], baseada em padrões de acesso e consumo, e até mesmo influir no hábito do usuário da internet, escolhendo o que mostrar e o que não mostrar, capitalizando também em cima disto (e até mesmo influenciando o resultado de processos políticos, como sugerem certos estudiosos[208]).

Através destas ferramentas, descobrem-se nichos de consumidores, separados de acordo com determinados critérios. Desta forma, as redes sociais e os negócios de tratamento de dados acabam por vender "pacotes" de publicidade dirigida aos anunciantes, baseados nas preferências e comportamento dos usuários das redes sociais; suas tendências políticas, gostos musicais, *hobbies*, atividades que realizam junto com grupos de amigos — todo dado e informação torna-se potencialmente aproveitável nesta perspectiva.

É neste panorama que se encontram os dados pessoais – aqueles que, de alguma maneira, podem ser relacionados a uma pessoa ou minimamente identificáveis e que, portanto, podem ser protegidos por certa esfera de privacidade.

Mostra-se muito interessante a utilização destes dados e informações como verdadeiros insumos e matérias primas[209] na realização de novos modelos de negócio, uma vez que se afiguram renováveis e crescentes em quantidades colossais dia a dia. Monetizá-los significa promover o desenvolvimento econômico, construindo negócios rentáveis[210]. Para os usuários, os dados acabam

adequadamente compreendidos por pessoas". TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de., op. cit., p. 124

[207] "A publicidade comportamental online constitui uma prática que consiste em direcionar anúncios publicitários específicos para determinados consumidores, de acordo com o seu comportamento online anterior, ou seja, é destinada a um grupo, classe ou categoria de consumidores de acordo com uma base de dados a respeito dos mesmos elaborada a partir de interesses previamente demonstrados. Deste modo, os fornecedores conseguem cada vez mais alinhar seus anúncios publicitários em relação aos supostos interesses de seus destinatários. De fato, a prática em questão consiste em uma espécie de segmentação de mercado fundamentada em um critério comportamental." ALVES, Fabrício Germano. **Análise da possibilidade de regulação da publicidade comportamental (behavioral advertising) pelo microssistema consumerista**. Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo. Brasília, v. 2, n. 1, p. 208-223, Jan/Jun. 2016. p. 214

[208] Frederike Kaltheuner, da Privacy International, e Michal Kosinski, professor da Universidade de Stanford, sugerem que as ferramentas de *Big Data*, mormente as utilizadas pela companhia Cambridge Analytica, tenham influeciado no resultado do Brexit (saída do Reino Unido da União Europeia) e da eleição norte-americana, vencida por Donald Trump. Cf.: DOWARD, Jamie; GIBBS, Alice. **Did Cambridge Analytica influence the Brexit vote and the US election?** Disponível em: <https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump>. Acesso em: 09 abr. 2018., e GRASSEGGER, Hannes; KROGERUS, Mikael. **How Cambridge Analytica used your Facebook data to help the Donald Trump campaign in the 2016 election**. Disponível em: <https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win>. Acesso em: 09 abr. 2018.

[209] "A primeira característica do novo paradigma [da tecnologia da informação] é que a informação é a sua matéria-prima: são tecnologias para agir sobre a informação, não apenas informação para agir sobre tecnologia, como foi o caso das revoluções tecnológicas anteriores. O segundo aspecto refere-se à penetrabilidade dos efeitos das novas tecnologias. Como a informação é uma parte integral de toda atividade humana, todos os processos de nossa existência individual e coletiva são diretamente moldados (embora, com certeza, não determinados) pelo novo meio tecnológico. A terceira característica refere-se à lógica de redes em qualquer sistema ou conjunto de relações, usando essas novas tecnologias da informação." CASTELLS, op. cit., p. 108

[210] "Cabe lembrar que a rede social virtual configura um modelo de negócio bastante rentável, embasado em conceitos como visibilidade, vigilância, identidade e indexação. Sua estrutura apresenta duas fases principais. Em primeiro lugar,

por funcionar como uma espécie de moeda de troca[211]: é possível usufruir de certos serviços aparentemente gratuitos, sem o pagamento de custos e taxas – mas o financiamento deste usufruto se dá através justamente da coleta dos dados pessoais.

Assim, serviços como o *Facebook, WhatsApp, Google* e redes sociais em geral utilizam os dados pessoais de seus usuários[212] como insumos para seus negócios, aproveitando quase todo o dado produzido: isto inclui as mensagens entre usuários, o conteúdo publicado em "grupos", as fotos, posições geográficas, o conteúdo de e-mails, entre vários outros dados; alegam[213] tais empresas que tomam precauções para que os dados pessoais circulem somente entre seus servidores e sistemas, mantendo, de tal forma, certa garantia de proteção aos dados pessoais e da privacidade de seus usuários.

Tal utilização dos dados com fins econômicos, contudo – sobretudo em se tratando das redes sociais[214] – suscita, como vem se demonstrando, forte preocupação[215] para com a privacidade dos usuários da internet e de seus serviços. São dados que são colhidos, não raro, sem o devido consentimento dos usuários, que também ignoram o destino de tais dados e o que deles será feito[216].

---

visa-se alcançar uma massa crítica de usuários e, posteriormente, parte-se para a exploração e a monetização da rede social, por meio da venda de espaços para a publicidade, da comercialização de produtos (como publicações patrocinadas) e da "venda" de perfis, cadastros e dados pessoais de seus usuários". TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de., op. cit., p. 122

[211] "So stellen Firmen wie Facebook und Google ihre Dienstleistungen scheinbar umsonst zur Verfügung und der Nutzer bezahlt mit seinem Nutzungsprofil. Dies ist ein sozialer Tausch, bei welchem zunächst kein Geld fließt. Monetäre Anreize entstehen erst auf der nachgelagerten Ebene, wenn die Informationen vom betreffenden Unternehmen beispielsweise zu Werbezwecken an Dritte verkauft werden." Em tradução livre, "Por exemplo, empresas como o Facebook e o Google parecem estar oferecendo seus serviços gratuitamente, mas os usuários estão pagando com seus perfis. Esta é uma troca em que inicialmente não flui dinheiro. Os incentivos monetários surgem apenas se, por exemplo, tais informações forem vendidas pelas empresas à terceiros com fins publicitários." JENTZSCH, Nicola. **Monetarisierung der Privatsphäre**: Welchen Preis haben persönliche Daten? Deutsches Institut für Wirtschaftsforschung Wochenbericht, n. 34, ago./2014, pp. 793-798. Disponível em: <https://www.diw.de/documents/publikationen/73/diw_01.c.479821.de/14-34-3.pdf>. Acesso em: 20 jun. 2018. p. 794.

[212] Informações de fácil constatação ao acessar as políticas de privacidade dos referidos serviços, disponíveis em: <https://www.facebook.com/privacy/explanation>; <https://www.google.com/intl/pt-BR/policies/privacy/>; e <https://www.whatsapp.com/legal/?l=pt_br>. Acesso em: 17 out. 2017.

[213] "Um grande problema, com relação ao fornecimento de informações on-line a empresas, diz respeito à forma como elas vão proteger esses dados. Muitas delas explicam nos sites, em termos gerais, a política de uso e proteção de informações dos clientes. Embora possam fornecer explicações básicas, não há detalhes, como que tipo de informação é criptografado ou como os funcionários são treinados para garantir que os dados pessoais não sejam impressos ou perdidos". CHERRY, Denny, op. cit., p. 6.

[214] "A utilização das redes sociais virtuais modificou profundamente a forma de obtenção, tratamento e divulgação de dados pessoais, o que impactou diretamente a própria expectativa de privacidade da pessoa humana. Nos dias atuais, dificilmente o indivíduo poderá alcançar um alto grau de controle sobre as suas informações e características pessoais depois que as inserir na rede. Dessa forma, pode-se afirmar que a velocidade da circulação da informação é inversamente proporcional à capacidade de seu controle, retificação e eliminação.". TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de., op. cit., p. 122

[215] "Dentro da lógica cética, muitos temem que a internet possa ser instrumento utilizado contra a privacidade e os direitos humanos, uma vez que a privacidade na internet não existiria nem para os governos e empresas e nem mesmo para os indivíduos". SUPPO, Hugo Rogelio. Internet e democracia. In: THEMOTEO, Reinaldo J. (Org.). **Cadernos Adenauer XVI, nº 3**: Internet e sociedade. Rio de Janeiro: Fundação Konrad Adenauer, 2015. pp. 19-45. p.31

[216] "Although contract law can protect privacy within relationships formed between parties, it does not redress privacy invasions by third parties outside of the contractual bonds. […] Today, our personal information is increasingly obtained by people and organizations that have never established any relationship with us". SOLOVE, op. cit., p. 81

As soluções ante a esta problemática são necessárias não apenas para a salvaguarda deste direito dos titulares dos dados pessoais, mas também para a segurança jurídica das empresas que atuam no ramo e para a sua competitividade[217].

Como se pôde adiantar, os dados, para muitos, são considerados o novo "petróleo", no sentido de sua potencialidade e valorização econômica. De forma a situar o trabalho em termos práticos, elencaremos, neste ponto, alguns exemplos de modelos de negócio que monetizam os dados pessoais[218] neste panorama[219], relacionando-os com algumas problemáticas surgidas desta prática; desta forma, tencionamos exemplificar os pontos de luz existentes na analogia sugerida (em termos de luz e sombra) para a conformação da privacidade como direito – como o elemento necessário ao preenchimento do seu conteúdo protetivo.

Assim, na sociedade em rede, são inúmeras as possibilidades propiciadas pelo avanço exponencial, nos últimos anos, do uso da internet[220] e das ferramentas em tratamento de dados: seja por soluções de *big data*[221] – como já adiantado, cenário de tratamento de grandes volumes de dados, de enorme variedade e em velocidades excepcionais[222] –, por meio de algoritmos, ferramentas de *business inteligence* ou de *machine learning*, o tratamento de dados para geração de

---

[217] "No início de 2018, houve bastante discussão sobre como os dados dos usuários estavam sendo utilizados por empresas que controlam sites de mídias sociais, que – como outras plataformas digitais – coletam enormes volumes de informações que são analisadas e monetizadas ao serem vendidas para serviços publicitários. A privacidade de dados está no cerne do debate. O uso de plataformas digitais tem crescido rapidamente em países em desenvolvimento, que também terão de se preocupar com essa questão. Quase 60 países em desenvolvimento não possuem uma legislação vigente que trate da proteção de dados. É fundamental mudar essa situação, não só para proteger os mais de 400 milhões de usuários do Facebook nesses países, mas, também, para assegurar que as empresas dessas nações possam se envolver em comércio efetivo com parceiros como a União Europeia, que tem imposto exigências rigorosas nessa área". FREDRIKSSON, op. cit., p. 37

[218] Em retrospecto, o Decreto nº 8.771/2016, regulador do Marco Civil, em seu art. 14, I, assim como o art. 5º, I, da LGPD, os define como qualquer dado relacionado à pessoa natural, identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa. Exemplos destes dados são: e-mails, mensagens, fotos, vídeos, coordenadas de GPS em tempo real; nossos interesses em diferentes temas, como música, cinema, esportes, política e religião; nossos hábitos de navegação, em quê clicamos, o quê compramos, quanto tempo passamos em determinados sites, dentre outros.

[219] Seja qual for sua nomenclatura, sociedade informacional, sociedade em rede, ciberespaço ou convergência digital, o certo é que vivenciamos, de fato, um paradigma cada vez mais dependente da informação e dos seus fluxos. Assim defende Tim Wu: "Embora a afirmação possa parecer banal, nós realmente vivemos numa sociedade e numa economia baseadas na informação. Nosso passado dependia muito menos da informação que o presente, e essa menor dependência foi utilizada por diversas indústrias da informação. Nosso futuro, contudo, deverá intensificar a realidade presente: uma dependência cada vez maior de informação em todas as questões relativas à vida e ao trabalho, e toda essa informação necessária viajando por uma só rede, que chamamos de internet". WU, 2012, op. cit., não paginado (epub).

[220] "[a] arquitetura interna da Internet é um ambiente propício à coleta, acúmulo e tratamento de informações pessoais. Essa conjuntura impõe severos riscos a uma série de direitos fundamentais, tais como o direito à privacidade e à proteção de dados". BIONI, op.cit., p. 172

[221] O conceito de Big data pode ser condensado como a busca em extrair inteligência dos dados e traduzi-la em vantagens comerciais; com dados que podem surgir na forma de mensagens, atualizações e imagens postadas em redes sociais; de leituras de sensores; sinais de GPS de celulares, etc. MACAFEE, Andrew; BRYNJOLFSSON, Erik. **Big Data**: The Management Revolution. Harvard Business Review 90 (10), p.60-68. October 2012. Disponível em: <http://goo.gl/SmDmfp>. Acesso em: 15 nov. 2017. p. 62-63.

[222] TEFFÉ; MORAES, op. cit., p. 124

receita já é uma realidade[223]. Assim, tais serviços criam e mantêm seus modelos de negócio com base nos dados e na informação, tendo estes ativos papel fundamental neste cenário[224].

No âmbito das redes sociais, o exemplo mais conhecido e difundido é o da publicidade dirigida[225], pelo qual os usuários, a partir da análise de seus dados pessoais, recebem propagandas de acordo com seu perfil. O *Facebook* é pródigo neste sentido, acumulando pouco mais de 2 bilhões de usuários e deles coletando inúmeros e diferentes tipos de dados[226], visando, essencialmente, vender anúncios[227].

São negócios, como se vê, bastante propícios[228] no atual quadrante, de exponencial avanço e democratização[229] tecnológica: são modelos que podem demandar, para sua realização, algum conhecimento em informática e programação, investimento baixo (para prover conexão com a internet e, se necessário, aluguel de servidor) e acesso aos dados, que, como é notório, são corriqueiramente utilizados como moedas de troca. Stuart Sumner, na obra com o sugestivo título "*You: for sale – protecting your personal data and privacy online*" (Você: à venda – protegendo seus dados pessoais e privacidade *online*, em tradução livre) explica que os serviços aparentemente livres de ônus financeiros que utilizamos *online* não são de todo gratuitos[230]; nós os pagamos com

---

[223] CHERRY, op. cit., p. 2-3.

[224] "A produtividade e a competitividade na produção informacional baseiam-se na geração de conhecimentos e no processamento de dados. A geração de conhecimentos e a capacidade tecnológica são as ferramentas fundamentais para a concorrência entre empresas, organizações de todos os tipos e, por fim, países". CASTELLS, op. cit., p. 165

[225] Fabrício Germano Alves conceitua a publicidade dirigida como "uma prática que consiste em direcionar anúncios publicitários específicos para determinados consumidores, de acordo com o seu comportamento *online*". Cf.: ALVES, op. cit., p. 214

[226] "A empesa armazena uma enorme quantidade de dados dos usuários. Além das informações do perfil e postagens, armazena metadados como data e horário de conexão, dispositivo utilizado, endereços IPs de onde conectou, informações do navegador, cookies armazenados, "cliques" realizados – assim como dia/hora e número de vezes, tópicos dirigidos ao usuário associado aos gostos e interesses do timeline, apps que utiliza, todas as conversas de chat realizadas, todos os likes dados, os compartilhamentos feitos, todas as fotos e vídeos postadas e seus metadados, grupos que participa ou participou, todas as pessoas que clicaram like em lugares, eventos, cidades que você logou, todas as buscas que realizou no site, os amigos que você removeu da conta e uma série de outras informações, mesmo que você já as tenha deletado (Facebook, 2015). O Facebook praticamente não apaga do que foi publicado e registra as interações feitas na plataforma da empresa, seja de forma ativa ou passiva". MACHADO; MORETTO, op. cit., p. 117

[227] "A então recém-criada empresa de Zuckerberg soube competir muito bem nesse recém-criado mercado baseando-se em um modelo de negócios profundamente consistente com o novo paradigma da web. O principal recurso do Facebook é sua plataforma na web aonde, de um lado, usuários podem manter-se conectados com amigos, família e demais conhecidos, manterem-se informados e se expressarem, e de outro, empresas parceiras podem vender anúncios direcionados ao público-alvo, manter páginas institucionais e engajar seus consumidores na divulgação de sua marca. Seguindo o modelo da web 2.0, o valor da empresa provém do conteúdo produzido tanto pelos próprios usuários quanto pelas empresas parceiras. O efeito rede, que faz com que quanto mais usuários mais valiosa seja a aplicação, associada ao duplo engajamento promovido pela plataforma, colocou o Facebook em uma posição bastante favorável na corrida pela base de dados mais cobiçada da web: as preferências pessoais e a rede de contatos dos usuários". Ibidem, p. 116

[228] TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de., *op. cit.*, p. 122

[229] Interessante trabalho do jornalista Romulo Tondo, de título "Smartphones e pobreza digital: o consumo de telefones celulares e internet por jovens de camada popular" faz uma abordagem que demonstra a capilarização e democratização do acesso à internet e seus conteúdos. Disponível em: <http://coral.ufsm.br/congressodireito/anais/2015/5-12.pdf>. Acesso em: 15 set. 2017.

[230] SUMNER, Stuart. **You: for sale** – protecting your personal data and privacy online. Waltham: Elsevier, 2016. p. 4

nossos dados pessoais, que podem, facilmente, ser explorados[231] e potencialmente violar aspectos da vida íntima e privada de seus titulares.

Outro exemplo de monetização de dados pessoais advém da venda de dados e de bases de dados. Existem inúmeras empresas especializadas neste nicho[232], fornecendo a outros "*data brokers*"[233] (corretores de dados, em tradução livre) pacotes de dados diferenciados (seja por etnia, por idade, por localização geográfica, por preferências, etc)[234] e ressignificados/trabalhados, e nem sempre com finalidade de publicidade. São utilizados, por exemplo, para aumentarem algumas já imensas bases de dados, tornando-as mais completas, mais fidedignas.

A coleta e tratamento de dados pessoais são usados, ainda – para além de conhecer melhor os possíveis e eventuais consumidores –, com vistas a conseguir vantagens competitivas e "*insights*" sobre os concorrentes de determinado nicho comercial[235].

Dito isto, passamos a exemplificar certas preocupações surgidas com o uso dos dados pessoais.

---

[231] SUMNER, *op. cit.*, p. 6

[232] "Várias empresas realizam o chamado data mining, coletando dados em larga escala para posteriormente vender essas bases de dados para terceiros. Além disso, na lista de empresas que colaboraram com a NSA constam diversas das maiores empresas da web e consequentemente do mundo". THEMOTEO, Reinaldo J. Cibercultura e participação política no Brasil. In: _____ (Org.). **Cadernos Adenauer XVI, nº 3**: Internet e sociedade. Rio de Janeiro: Fundação Konrad Adenauer, 2015. pp. 7-17. p. 13

[233] "After obtaining public data, people-search sites sprinkle in phone book information, details from marketing lists, commercial records, and other information. Through such documents, data brokers know where you live and have lived, your phone numbers—often including cell phone—your neighbors and relatives, educational history, past lawsuits, bankruptcies, criminal history, and many other details. The data broker websites mix all this information together, much as a food manufacturer pours twenty-five ingredients into a batch that becomes a packaged snack. Think Cheez Whiz. Once the Cheez Whiz glops onto your plate, there's no telling where its ingredients originally came from. […] Today Inflection spends between $3 million and $5 million a year to buy and rent the personal data that appear on PeopleSmart.com. Inflection relies on ten to fifteen companies for the bulk of its personal data, with another ten to fifteen adding supplementary information such as educational backgrounds and criminal records. Confidentiality agreements bar Inflection from naming its suppliers, but they are among the big personal-data companies. Top players in the field include Acxiom, Epsilon, Experian, TransUnion, and Equifax, the latter three best known to the public for their credit bureau operations". TANNER, op. cit., p. 63

[234] "Sophisticated segmenting allows direct marketers to rent very specific lists. Among the countless variations on offer are Americans of Iranian, Albanian, or Vietnamese descent or other ethnic origins; contributors to AIDS research; male virility supplement buyers; depression medication users; and cancer victims. Also available: gays who own boats; recently divorced African Americans; tobacco chewers; rich baseball fans; birth control users; readers who buy books about drug and alcohol abuse; women who have bought porn or sex toys; concealed weapon permit holders; online gamblers; and subscribers to *The Dairy Goat Journal* (just 4,025 households at the beginning of 2014)". Ibidem, p. 76

[235] É o caso, por exemplo, do cassino "Caesar's Palace", de Las Vegas, nos EUA: "'Mastering data analytics, and customer data in particular, has given Caesars an edge in a business where rivals compete fiercely with the same games. […] By prospering on the backs of so much personal information, Caesars have inspired companies across the economy. Everyone wants to learn more about customers in hopes of marketing more successfully. Rivals closely watch to see what Loveman and Caesars will come up with next'". TANNER, op. cit., p. 18

3.2 PROBLEMÁTICAS RESULTANTES DA MONETIZAÇÃO DOS DADOS PESSOAIS

O cenário mensurado parece sugerir, de fato, que os dados possuem um intrínseco, inescapável e atraente aspecto econômico. Seriam, para alguns, "o novo petróleo". Esta metáfora, como já foi dito, soa até certo ponto adequada para o que se pretende no presente trabalho. Comparar a exploração dos dados com a indústria de petróleo e gás é fazer um paralelo com um setor que demonstra pouca ou quase nenhuma preocupação com as consequências de suas atividades exploratórias. É evidenciar os riscos que a exploração de determinada matéria-prima traz para o ambiente que o circunda.

A extração de petróleo é uma atividade extremamente nociva para o meio ambiente: quando produzido *off shore*[236], por exemplo, prejudica a população de animais marinhos em seu redor, através do descarte de água produzida, ruídos ou vazamento de absurdas quantidades de óleo cru – com impactos negativos duradouros na natureza. De igual maneira a queima de seus derivados, que promovem a poluição da atmosfera e contribuem para o efeito estufa[237].

Prosseguindo nesta metáfora, a exploração dos dados pessoais de uma maneira desmedida, sem limites e regulações, pondo a necessidade por lucro acima dos interesses da coletividade e de direitos fundamentais – à guiza da indústria petrolífera – pode igualmente ter consequências nefastas – mormente, e como têm se demonstrado ao longo do trabalho, com relação à privacidade dos usuários da internet.

Exemplos de como esta prática pode violar a privacidade são inúmeros: do clássico caso do pai que soube que seria avô de uma maneira inconveniente[238], ao do Facebook, que sugeriu para pacientes que frequentavam o mesmo consultório psiquiátrico que fossem 'amigos' na rede social[239], até a casos mais graves e preocupantes, como o de algoritmos de análise facial que podem predizer a sexualidade de usuários de uma rede social de encontros[240] e do uso dos dados pessoais coletados com fins de espionagem, controle e vigilância[241].

---

[236] CRUZ, Everton Lima da; CARVALHO, V. M. B. Recursos hídricos na indústria do petróleo e gás: a produção e o descarte de água em plataformas. In: XAVIER, et. al (org.). **Proteção do meio ambiente na indústria do petróleo e gás natural**. Natal: EDUFRN, 2016. p. 104

[237] MAIA; XAVIER, op. cit., p. 299-316.

[238] HILL, Kashmir. **How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did**. Disponível em: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#15478c546668>. Acesso em: 14 set. 2017.

[239] _____. **Facebook recommended a psychiatrist's patients friend each other — and there's no clear explanation**. Disponível em: <http://www.businessinsider.com/facebook-people-you-may-know-2016-8>. Acesso em: 14 set. 2017.

[240] LEVIN, Sam. **New AI can guess whether you're gay or straight from a photograph**. Disponível em: <https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph>. Acesso em: 14 set. 2017.

[241] BBC. **Edward Snowden: Leaks that exposed US spy programme**. Disponível em: <http://www.bbc.com/news/world-us-canada-23123964>. Acesso em: 14 set. 2017.

Este direito fundamental pode, portanto, ser violado diretamente, através do acesso não-autorizado aos dados pessoais (v. g., o vazamento da base de dados da Equifax[242]), como indiretamente, por meio da conjugação de diferentes tipos e quantidades de dados (como explicado por Fulgencio Madrid Conesa na alegoria do mosaico[243]).

Entretanto, a analogia com a indústria do petróleo não alcança o tamanho real do risco que o uso dos dados pessoais ostenta para a privacidade e os seus valores conexos; vazamentos de óleo, ainda que extremamente danosos, são passíveis de limpeza, de soluções emergenciais, contingenciais, para minimização dos danos. Isto não é verdade com os dados pessoais: o seu vazamento, seu destrato, mau uso ou uso negligente pode ter efeitos irreversíveis – imagine-se, por exemplo, a devassa de dados que revelem a sexualidade da comunidade homossexual de países muçulmanos, como Irã, Arábia Saudita ou Indonésia.

A prática de *surveillance* sobre os dados pessoais de cidadãos, captados por governos em nações, por exemplo, que vivem guerras civis e perseguições violentas à dissidentes e oposicionistas, ensejaria movimentos de repressão terrivelmente eficazes e sanguinários. A coleta de dados diversos através de *data mining* poderia tornar o acesso à saúde um direito muito mais caro e distante da realidade das pessoas, caso seus dados pessoais, conformando imagens da sua vida e da sua saúde, criem figuras – ainda que corretas ou incorretas – de sua disposição física e mental que padeçam de tarifas mais caras em planos de saúde[244] (ou mesmo seguros de vida).

Dados coletados com uma finalidade, mas utilizados de outra maneira, podem ter uma enorme influência na vida, na consciência e nas decisões das pessoas, ainda que elas não tenham completa noção disto – exemplos são os escândalos envolvendo o Facebook e a Cambridge

---

[242] MATHEWS, Lee. **Equifax Data Breach Impacts 143 Million Americans**. Disponível em: <https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#248efd3f356f>. Acesso em: 15 set. 2017.

[243] Em suma, seria a junção de diversas peças que, tomadas em separado, não possuem significado, mas que tidas em conjunto, conformam uma figura, um retrato, palpável e analisável. CONESA apud LEONARDI, op. cit., p. 74.

[244] "Alvo de investigação na Europa, onde atuava, a empresa Phorm encontrou no Brasil um mercado abundante, onde poderia dar prosseguimento às suas operações de rastreamento e monitoramento dos usuários da Internet. Aliou-se a duas empresas telefônicas, também provedoras de conexão à internet, e garantiu, assim, o acesso aos registros de atividades dos clientes: no que clicavam, fotos que visualizavam, vídeos a que assistiam, buscas feitas na rede... Tudo. Estas informações eram então usadas para marketing direcionado, um mercado que paga caro por informações precisas. Afinal, quanto vale para uma empresa que vende artigos esportivos, por exemplo, saber exatamente que produto oferecer a tal pessoa? Consumidores do provedor de conexão eram vítimas de um flagrante desrespeito à sua privacidade. Os clientes sequer tinham conhecimento de que seus dados eram coletados, processados e repassados a terceiros. A situação pode se agravar. Imagine uma pessoa que, preocupada com sintomas que vem sentindo, procura na internet informações sobre determinada doença. Recorre, então, a um plano de saúde. Mal sabe este internauta que a empresa já tem à disposição seus dados de navegação, pois fez um acordo comercial com o provedor. A seguradora, então, exige exames que verifiquem a existência da doença pesquisada, antes de estabelecer o preço do plano. O Marco Civil proíbe este tipo de prática, assegurando o sigilo da navegação do internauta: 'é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados'. O direito à inviolabilidade da intimidade e da vida privada também estão garantidos, conforme estabelecido no Artigo 7º". MOLON, Alessandro. A legislação e a internet. In: THEMOTEO, Reinaldo J. (Org.). **Cadernos Adenauer XVI, nº 3**: Internet e sociedade. Rio de Janeiro: Fundação Konrad Adenauer, 2015. pp. 97-112. p. 99-100

Analytica, acusados de terem sido mesmo responsáveis na mudança de curso de fluxos democráticos e cenários geopolíticos mundiais pela influência no Brexit e na eleição de Donald Trump nos EUA.

Assim, conformaremos, no tópico adiante, os valores sob ameaça neste cenário de potencial violação da privacidade, lançando as bases para a necessidade de regulação das práticas de monetização de dados pessoais.

3.2.1 Pontos de luz e valores conexos

Antes de aprofundarmos neste subitem, façamos, por força de didatismo, breve retrospecto do que até então defendemos: a privacidade, tida como direito humano e fundamental, encontra-se possivelmente ameaçada no âmbito do novo paradigma da sociedade em rede, paradigma que se sustenta (e se reproduz), cada vez mais, no protagonismo da informação e dos dados nos campos da economia, do comércio e até mesmo da política; positivado na Constituição e em outros diplomas legais nacionais, o direito fundamental à privacidade, por seu caráter abstrato e aparentemente vazio, requer, a nosso ver, a contextualização com casos concretos para conformar seu conteúdo protetivo – dessa forma, transparece os valores que lhe são conexos, baseados na qualidade perene da liberdade (que se desdobra em liberdade política, de consciência, de expressão, religiosa, no livre desenvolvimento da personalidade, etc); como equação para fazer surgir o conteúdo protetivo da privacidade neste panorama e respeitando os argumentos elencados (precipuamente a liberdade), sugerimos a metáfora em termos de luz e sombra, no qual a sombra representa os aspectos tutelados pela privacidade que, livremente e *pari passu*, modela-se aos pontos e focos de luz – estes, por sua vez, representando os interesses que ostentam possíveis riscos de violação à privacidade e seus valores.

Os dados pessoais, destarte, inseridos neste cenário de sociedade em rede e à mercê das técnicas e soluções tecnológicas adequadas ao seu uso, tratamento e monetização – permitimo-nos dizer, por quê não, à mercê do seu refino, tal qual matéria prima –, carregam consigo o potencial de conformação de aspectos íntimos e privados dos seus titulares, sendo, por isso e a nosso ver, a sua proteção corolária do direito fundamental à privacidade.

Assim, é possível estabelecer uma clara conexão entre as práticas de monetização de dados pessoais com potenciais violações da privacidade e valores conexos. Com o intuito de demonstrar a necessidade de regulação das práticas monetizantes dos dados pessoais, elencaremos adiante certos pontos que consideramos cruciais para a manutenção dos valores protegidos pelo direito fundamental à privacidade.

A tabela a seguir expõe em termos mais perceptíveis e práticos o resumido acima:

Âmbito	**Valores conexos**	**Direitos e Princípios relacionados**	**Aspectos de risco do uso de dados**	**Elementos que originam riscos/Focos de luz**	**Perigos**	**Estratégias de mitigação de danos/riscos**
Social	Igualdade	Não discriminação; Desenvolvimento da personalidade	Classificação Preconceito Discriminação	Grandes quantidades de dados	Discriminação	Minimização de coleta de dados / atinência aos princípios reguladores
	Solidariedade	Igualdade entre gêneros	Segregação social Discriminação Menor acesso à políticas serviços	Dados sensíveis		Supressão de elementos sensíveis Mais controle popular sobre práticas de *surveillance*
	Justiça social	Acesso à previdência e assistência social		Preconcepções/preconceitos nos bancos de dados		Remoção de preconcepções dos bancos de dados
		Acesso à serviços de saúde		Uso de algoritmos discriminatórios		Programação de algoritmos precavidos contra a discriminação
						Reformular os resultados da prática de *profiling*
Político	Liberdade	Liberdade de pensamento, consciência, ideológica, religiosa	Exclusão/ normalização de grupos distintos; perseguição política;	Falta de transparência; Visibilidade e não-verificabilidade da *surveillance*	Autovigilância e autocensura por receio de estar sendo vigiado	Maior transparência; Mais adoção de práticas de *privacy by design*
	Participação	Liberdade de reunião e associação				
	Democracia					

Figura 1: Quadro demonstrativo das correlações entre os âmbitos, valores, direitos, princípios, uso de dados, perigos e estratégias de minimização de riscos no cenário da monetização de dados. Adaptado e traduzido de: ORRÙ, Elisa. Minimum Harm by Design: Reworking Privacy by Design to Mitigate the Risks of Surveillance. In: LEENES, Ronald, et. al. (ed.). **Data Protection and Privacy**: (In)visibilities and Infrastructures. Dordrecht: Springer, 2017. pp. 107-138. p. 132

Como se pode ver, a proteção de dados pessoais, tida no âmbito protetivo da privacidade e contextualizada na sociedade em rede – com todas as suas práticas, tecnologias e técnicas – é um tema deveras complexo[245], que envolve uma numerosa gama de interesses, agentes, atores, direitos,

[245] "[…] the present contribution advances the thesis that data protection is by its nature an extraordinarily complex field and therefore requires multi-level and complex regulation. Yet at its core, the legal framework is still characterized by out-dated concepts going back to when data protection first emerged. This applies both to the understanding of

princípios, valores, riscos e perigos. A abordagem de quem deseja tratar deste tema, inevitavelmente, recai em um esforço multidisciplinar – não raro, com nuances inovadoras, vanguardistas e ousadas. Afinal, são problemáticas novas, desafiadoras, que apresentam perspectivas intensamente complexas, mesclando temas como tecnologia, economia, sociologia, filosofia e direito.

Acreditamos ser possível discernir, entre os estudiosos da temática e pelo que até então se expôs, duas posições bem distintas: há aquelas visões que, confiantes nas benesses da tecnologia e na força do arcabouço normativo, acreditam que é possível colher os frutos positivos da técnica sem temer as vilanices propiciadas pela mesma, já que o Direito estaria equipado e capacitado a enfrentar os desafios surgidos – é uma postura que se pode chamar de otimista (ou ingênua, para a próxima visão); de outro lado está aquela visão que, constatando o vigor, liberdade e impositividade da técnica ante a debilidade, vagarosidade e inadequação da Lei em se adaptar, tomam por perdida a batalha na defesa dos direitos, liberdades, valores e prerrogativas postos em xeque pela monetização de dados pessoais – postura que podemos chamar de pessimista (ou derrotista, para a primeira postura).

Não com certo receio (e também ressalvas), o trabalho se alinhamo à posição do primeiro grupo, o dos otimistas, por acreditar que a batalha pela proteção dos direitos, como queria Bobbio, é escaramuça possível e necessária – sobretudo quando nos despojamos da ideia derrotista de falência dos Códigos ante as linhas de códigos, do Estado ante os fluxos, da Lei ante a técnica. Por quê estes conceitos têm de andar separados? Por quê tem de serem afastados? Por quê não podem ser tomados em uma perspectiva conciliadora, mescladora, inovadora?

Defende-se que, em vez de acusar a derrota do Estado, a sua incapacidade e deficiência no paradigma da sociedade em rede, deve-se adotar uma postura que busque integrar o Estado à rede com a finalidade de imprimir a maior força normativa possível às suas leis e seus princípios, assim como agarrar tanto quanto poder fiscalizatório e sancionatório o possível[246]: adota-se uma postura maquiavélica[247] neste sentido – para nós, o importante (como bem apontamos no início do trabalho,

fundamental rights relevant to data protection and to the basic approaches to regulation. Modern data protection calls for new legal approaches". ALBERS, Marion. **Realizing the Complexity of Data Protection**. In: GUTWIRTH, et. al. (eds.), op. cit., 2014, p. 213

[246] "In considering, specifically, conditions under which informational norms may warrant explicit expression and enforcement through law and public policy, I would suggest those in which violations are widespread and systematic, when the parties involved perpetrating the violations are overwhelmingly more powerful or wealthy and moved by pure selfinterest. In such situations, the violations take on public signifi cance and call for public response". NISSENBAUM, 2010, op. cit., p. 237

[247] "Segundo Cortez, porém, a opção preferencial por instrumentos de regulação fraca pode levar a uma regulação subótima no longo prazo. O regulador, diz, não deve ficar hesitante e abdicar de usar ferramentas coercitivas diante de novas tecnologias. Se houver preocupação com a prematuridade da regulação, pode optar por mecanismos alternativos de coercibilidade, mas, arremata, 'o interesse público demanda que as agências mantenham a sua força diante da disrupção regulatória'". BAPTISTA, Patrícia; KELLER, Clara Iglesias. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. **RDA – Revista de Direito Administrativo**, Rio de

como pressuposto metodológico crítico) é a salvaguarda dos direitos fundamentais, mormente o da privacidade, não importando os meios para tanto; vírgula que destacamos neste momento é a da delimitação do papel estatal nessa propositura – queremos, aqui, defender um Estado-escudo, um Estado-garantidor, e não um Grande Irmão orwelliano ou um *panopticon* benthamniano[248].

Defende-se aqui um Estado que reflita as ânsias da população que, situada entre o fogo cruzado dos grandes interesses em fluxo na sociedade em rede, pouco ou quase nenhum poder e eficácia possuem para fazer valer suas vontades[249]. Afinal, se a isto não se presta o Estado[250], viver em sociedade já de nada serve.

Sem embargo, parte-se do pressuposto que o Estado, no âmbito da sociedade em rede, é, ainda, no espectro dos nós que conformam as redes, um dos últimos *locus* de debates, consenso e construção democrática de leis, princípios e direcionamentos da sociedade: em um Estado Democrático de Direito, em que há separação de poderes, respeito aos direitos, prerrogativas e deveres do cidadão, e no qual a produção legislativa (geralmente realizada por meio de sistemas representativos) deve (ou deveria) refletir as ânsias, interesses e direitos do povo, existe, pois, a possibilidade de atuação do Estado como um nó influente na costura das redes, representando os indivíduos.

Há quem diga que a internet, pela sua capacidade inata de conectar e ligar as pessoas de uma maneira nunca antes vista, substituiria os velhos modos de fazer política[251] e, consequentemente, de

---

Janeiro, v. 273, p. 123-163, set./dez. 2016. p. 155

[248] Estes exemplos denotam um ente centralizador, ubíquo e onisciente, capaz de vigiar a tudo e a todos, a qualquer tempo; não é isto que propomos, já que, na nossa visão, o Estado atuaria como fiscalizador através de uma autoridade reguladora, e não como coletor de dados pessoais com fins de vigilância ou intentos ditatoriais. Aqui, importa mencionar a origem do panopticon como sendo uma espécie de prisão, visionada por Jeremy Bentham, na qual, pela sua disposição (celas em disposição circular mirando o centro do pátio, que contém uma única torre de observação, redonda – sem que os encarcerados saibam se há ou não um guarda a lhes vigiar), estimularia uma vigilância ubíqua e constante, na qual a mera sensação de se estar sendo vigiado compeliria o encarcerado a obedecer as normas impostas. Não são poucas, inclusive, as críticas à alusão desta metáfora até mesmo para ilustrar o cenário da vigilância. Por exemplo, conferir: "The panopticon refuses to go away. Despite the appearance of a number of critiques (e.g. Bauman 1992; Bogard 1996; Lyon 1993; Mathiesen 1997), the idea of the panopticon still appears routinely in surveillance discourses." LYON, David. **Theorizing Surveillance**: The panopticon and beyond. Cullompton: Willan, 2006. p. 4; "Há limites históricos, assim como lógicos, à utilização das imagens do pan-óptico hoje." BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Trad. Carlos Alberto Medeiros. Zahar: Rio de Janeiro, 2014. p. 55

[249] Claro exemplo disto são os contratos de adesão impostos pelas redes sociais, nos quais o consumidor, em uma lógica de all-or-nothing (tudo ou nada): ou se aceita os termos como impostos, ou não se usufrui do serviço oferecido pela rede social em questão.

[250] "Rooted in the classic writings of noted social contractarian philosophers and reflected more recently in the work of John Rawls, social contract theory provides that 'rational individuals will agree by contract, compact, or covenant to give up the condition of unregulated freedom in exchange for the security of a civil society governed by a just, binding rule of law'". BIEGEL, Stuart. **Beyond our control?** confronting the limits of our legal system in the age of cyberspace. Cambridge: MIT, 2001. p. 101

[251] "A participação política possibilitada pelas TIC tem sido considerada como uma das promessas da internet. No entanto, os resultados […] têm sido muito modestos. A participação tem quer entendida no contexto da contemporaneidade, onde se tem detectado um abandono ou desvalorização da política. 'A política está em crise tanto por força de uma situação objetiva, estrutural, quanto por força da ativação de projetos ideológicos bem específicos e da dissolução, ainda que relativa, das utopias fundamentais da modernidade'" PINHO, José Antonio Gomes de. **Sociedade da informação, capitalismo e sociedade civil:** reflexões sobre política, internet e democracia na realidade brasileira.

produzir (e fazer valer) o Direito. Todavia, não é o que se observa, sobretudo quando se considera os casos já mencionados do Brexit e da eleição de Donald Trump; recaem suspeitas, inclusive, de influências estrangeiras em tais processos democráticos, suscitando inevitavelmente a reflexão sobre o papel e o peso que as redes possuem nos processos políticos. Qual ideologia está se permeando pelas redes[252]? A quem serve a utilização dos dados pessoais de seus titulares? Com quem concordamos, sem ao menos ter ideia de que o fazemos? É inegável, e cada vez mais nítida, a importância e protagonismo que a informação, surfando na tsunami que é a internet, possui na sociedade hodierna[253].

É nessa esteira, inclusive, que mencionamos o notável trabalho de Yuval Noah Harari. Na obra "Homo Deus: uma breve história do amanhã", este historiador israelense debulha o conceito que aludimos no capítulo anterior, o "dataísmo"[254]. Em apertada síntese, o dataísmo seria a "religião dos dados", no sentido de ser uma "fé"[255], uma crença na capacidade de conversão de todo e qualquer aspecto da vida – não só humana – em uma linguagem simples de códigos decifráveis, tratáveis e reproduzíveis; fundamentalmente baseado na biologia e na informática, este conceito prediz a inevitável conversão de toda vida humana em códigos e algoritmos.

Assim, como exemplifica Harari, o capitalismo ou o socialismo seriam apenas modos[256] de entender códigos econômicos – seriam algoritmos distintos debruçando-se sobre um mesmo material, apenas formas diferentes de organizar os dados. Os constructos sociais, tais quais o casamento, amizades, inimizades, entre outras convenções sociais, seriam simplesmente algoritmos

---

RAE, São Paulo, v. 51, n. 1, jan./fev. 2011, pp. 98-106. p. 101

[252] "É uma verdade incontestável, embora não reconhecida, que, assim como você é o que come, o que você pensa ou a maneira como pensa dependem da informação a que estiver exposto. Como você ouve as vozes dos líderes políticos? De quem é a dor que você sente? De onde vêm suas aspirações, seus sonhos de uma vida boa? Tudo isso provém de um ambiente de informação." WU, 2012, op. cit. não paginado.

[253] "Ainda que não sejam óbvias de imediato, essas questões mais profundas estão de fato no cerne da batalha que se trava sobre o futuro da internet. Ao analisar esses problemas na perspectiva do século XXI, surge uma realidade óbvia e surpreendente: a informação se tornou excepcional como categoria industrial mesmo em relação à história da própria indústria. Uma única rede universal transporta não só algumas coisas, mas todas as coisas: voz, vídeo, notícias, cultura e comércio". Ibidem, não paginado.

[254] "De acordo com o dataísmo, a Quinta Sinfonia de Beethoven, uma bolha no mercado de ações e o vírus da gripe são apenas três padrões de dados cujos fluxos podem ser analisados por meio dos mesmos conceitos básicos e das mesmas ferramentas. Essa ideia é extremamente atraente. Ela oferece a todos os cientistas uma linguagem comum, constrói pontes sobre brechas acadêmicas e exporta facilmente insights através de fronteiras disciplinares. Musicólogos, cientistas políticos e biólogos celulares podem finalmente se entender". HARARI, op. cit., não paginado.

[255] "Quando você está considerando com quem deve se casar, que carreira seguir, ou se deve começar uma guerra, o dataísmo lhe diz que seria total perda de tempo escalar uma montanha elevada e contemplar o pôr do sol sobre as ondas. Seria igualmente irrelevante ir a um museu, escrever um diário privado ou ter uma conversa íntima com um amigo. Sim, para poder tomar as decisões corretas, você precisa se conhecer melhor. Mas, se quiser se conhecer melhor no século XXI, existem métodos muito melhores do que escalar montanhas, ir a museus ou escrever diários. […] os grandes algoritmos da internet de todas as coisas lhe dirão com quem casar, que carreira seguir e se é para começar uma guerra.". Ibidem, não paginado.

[256] "De acordo com essa visão, o capitalismo de livre mercado e o comunismo controlado pelo Estado não são ideologias, credos éticos ou instituições políticas que competem entre si. No fundo, são sistemas de processamento de dados que competem entre si. O capitalismo usa um processamento distribuído, enquanto o comunismo se fundamenta em um processamento centralizado". HARARI, op. cit., não paginado.

criados pela bioquímica humana com vistas a uma melhor taxa de sucesso de sobrevivência e manutenção da vida.

Neste universo de reducionismo aos dados, como se vê, tudo eventualmente poderia ser reduzido a códigos e dados. É um cenário, como bem alerta Harari, que confere a políticos e pessoas de poder capacidades inéditas de influência e exercício de dominação[257].

Tida nesta perspectiva, a monetização dos dados pessoais ostenta, como vem se defendendo ao longo do trabalho, inúmeros riscos à privacidade e aos seus valores conexos. Os pontos de luz da equação 'luz e sombra' começam a se discernir ante a miríade de nós, fluxos e vontades da rede.

É inegável que existem benesses no uso e no tratamento de dados pessoais: inúmeros são os serviços que facilitam a vida cotidiana e que fazem uso de nossos dados, como os aplicativos de mapas e trânsito. É possível imaginar, igualmente, que o uso de dados relativos à saúde dos titulares – dados considerados sensíveis – em estudos e pesquisas científicas, podem permitir *insights* e novas descobertas em termos de tratamento médico. É igualmente prático e agradável poder encontrar produtos especialmente direcionados aos nossos interesses, aproveitando descontos e promoções em itens que muitas vezes precisamos. Novos negócios surgem corriqueiramente, fundamentados nas inúmeras oportunidades que o tratamento de dados proporcionam.

A livre iniciativa, a liberdade de modelos de negócio e a livre concorrência, inclusive, são fundamentos e princípios protegidos e promovidos pelo Marco Civil da Internet, em seus arts. 2º[258] e 3º[259]. É inconteste que a sociedade informacional é âmbito que permite o desenvolvimento econômico, tecnológico e comercial, devendo estas possibilidades serem encorajadas e, ao máximo possível, não tolhidas.

Entretanto, e como se infere da leitura dos mesmos dispositivos aludidos, são também protegidos os direitos humanos, o desenvolvimento da personalidade, a garantia de liberdades e a proteção da privacidade e dos dados pessoais. São atividades que devem englobar e harmonizar

---

[257] "Para políticos, homens de negócio e consumidores comuns, o dataísmo oferece tecnologias inovadoras e poderes inéditos e imensos". Ibidem, não paginado.

[258] Art. 2o A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como: I - o reconhecimento da escala mundial da rede; **II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais**; III - a pluralidade e a diversidade; IV - a abertura e a colaboração; **V - a livre iniciativa, a livre concorrência** e a defesa do consumidor; e VI - a finalidade social da rede. [grifos nossos].

[259] Art. 3o A disciplina do uso da internet no Brasil tem os seguintes princípios: **I - garantia da liberdade de expressão, comunicação e manifestação de pensamento**, nos termos da Constituição Federal; **II - proteção da privacidade; III - proteção dos dados pessoais,** na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; **VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei**. Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. [grifos nossos].

estes princípios aparentemente conflitantes, sobretudo quando considerados os riscos que a monetização de dados pessoais oferecem.

São riscos inerentes ao próprio trato dos dados pessoais. Os pontos de luz são inúmeros, e podem atingir, volitiva ou negligentemente, aspectos protegidos pela privacidade e seus valores conexos. O livre desenvolvimento da personalidade encontra-se potencialmente em risco, já que os algoritmos, descobrindo mais sobre a vida dos titulares do que eles próprios, passam a retroalimentar os influxos iniciais (de preferências e posicionamentos) de um cidadão ou de uma coletividade; passa-se a viver em uma bolha, tendo-se contato apenas com aquilo que se tem preferência ou interesse. Qual o efeito disto em uma democracia? É possível ainda se falar em livre pensamento político, por exemplo, frente a estes riscos?

O Oráculo de Delfos é repaginado; não são mais necessários sacerdotes ou sacerdotisas para interpretar a vontade dos deuses e os seus interesses e desígnios para a vida dos cidadãos – agora, basta preencher seu *login* e senha, e pronto: os dados e algoritmos, em frenético transe, nos dirão o que ver, o que fazer, o que comprar, do quê gostar, do quê se afastar; eles nos separarão, classificarão e nos tangerão, tal qual em um curral 4.0. Liberdade de pensamento, liberdade política, liberdade ideológica, a democracia: são valores que, na conjuntura proposta, encontram-se em perigo ante a violação da privacidade.

Os dados pessoais, destarte, são a matéria-prima que permite estes problemáticos cenários. Não é exagerado afirmar isto: afinal, já Joseph Goebbels[260] exaltava o poder[261] político que a mídia possuía (e, em sua época, contentava-se com o rádio e o cinema). Qual seria sua animação ante uma ferramenta como a internet? Que futuro uma prática como esta, não regulada, ensejará?

O risco destas atividades, como vimos defendendo, é muito alto. Muitas liberdades estão em jogo quando se trata de dados pessoais e privacidade. Por esta razão é que argumentamos ser os dados pessoais não o 'novo petróleo', mas, sim, o 'novo urânio': tal qual um material radioativo, a prática de monetização de dados pessoais, apesar dos incontestáveis benefícios, necessitam de um extremo cuidado no seu trato, sob pena de violação de direitos fundamentais.

[260] "Here was the crowning achievement of the Reichsfunk-Gesellschaft, the National Radio Division of the Ministry of Public Enlightenment and Propaganda of the Third Reich. Its reach and power had caused Minister Joseph Goebbels to declare German radio the 'towering herald of National Socialism,' a force equal to creating a nation with 'one public opinion.' His broadcast chief bragged that 'with the radio we have destroyed the spirit of rebellion.' By means of this attention infrastructure, one man could at will reach the minds of the entire nation, whether they cared to hear him or not. As architect Albert Speer said at his war crimes trial, the Third Reich was the first dictatorship which made the complete use of all technical means for domination of its own country. Through technical devices like the radio and loudspeaker, 80 million people were deprived of independent thought. It was thereby possible to subject them to the will of one man'." WU, Tim. **The Attention Merchants**: the epic scramble to get inside our heads. New York: Alfred A. Knopf, 2016. Não paginado (epub).

[261] "Foi por isso que Joseph Goebbels definiu o rádio como 'a arma espiritual do Estado totalitário'. Por esse mesmo motivo, nos anos 1940, o regime nazista desenvolveu novas formas de mídia com a mesma intensidade que novas armas de destruição. Atrás de cada tirania ou genocídio há uma parceria silenciosa com algum tipo de mídia de massa". WU, 2012, op. cit., não paginado.

Assim é que, no próximo capítulo, elaboramos acerca da necessidade e possibilidade de regulação da monetização dos dados pessoais com vistas à proteção da privacidade e dos valores que ela engloba. É possível adiantar que defendemos uma perspectiva de regulação do risco, conforme já introduzimos, ao comparar os dados pessoais a um material radioativo. Serão propostas, ainda, perspectivas regulatórias frente a este cenário, sugerindo soluções, novas e velhas, capazes de abordar com eficiência a problemática estudada.

4 PERSPECTIVAS REGULATÓRIAS SOBRE O TRATAMENTO DE DADOS PESSOAIS NO BRASIL

No capítulo primeiro, o trabalho busca situar a acepção e o conteúdo do direito à privacidade; situar porque, como se viu, a sua conceituação se mostra tarefa tão complexa quanto possivelmente falível. Argumenta-se que, neste intento, a melhor saída é aquela que envolve a contextualização deste direito na busca pelo preenchimento de seu conteúdo protetivo.

No capítulo seguinte, apresenta o cenário no qual o direito à privacidade está inserido e pode ser contextualizado: o da sociedade em rede, que baseia-se na utilização dos dados e informações em seus diversos processos – não somente o econômico. Defende-se que os dados pessoais, insertos neste panorama, ostentam a capacidade de conformar aspectos da privacidade, traduzindo-se em potencial situação de violação das liberdades[262] inerentes àquele direito, sendo a monetização de tais dados, portanto, atividade que representa riscos às liberdades dos titulares dos direitos.

Neste capítulo, argumenta-se pela necessidade de regulação das atividades de monetização dos dados pessoais ante a precisão de se proteger a privacidade e as liberdades nela inclusas. Não exsurge, igualmente, como tarefa simples: a partir do que se expôs acerca da sociedade em rede, a governança[263] e regulação de uma rede de fluxos supranacionais[264] apresenta uma série de desafios, a começar pelo próprio papel do Estado.

Como aplicar, fiscalizar e realizar o *enforcement* de leis e normativas nacionais à empresas situadas em jurisdições geograficamente[265] distintas? Como fazer com que atores e agentes, em um contexto de rede, adéquem-se às normas e princípios estipulados pelo Estado nacional? A solução está em uma governança supranacional, baseada na cooperação? Ou talvez por meio da não regulação estatal, deixando a cargo dos próprios atores participantes da monetização de dados a

---

[262] "Privacidade e liberdade interligam-se intimamente. Não se assegura privacidade sem liberdade, o que se constata em regimes de exceção; e não se exercita liberdade sem privacidade, sendo esta indispensável à livre manifestação do pensamento, crença e expressão". VIEIRA, op. cit., p. 274

[263] "Assim, a governança consistiria em um fenômeno mais amplo do que o governo, de modo a abranger não apenas instituições governamentais, mas também mecanismos informais, de caráter não governamental, por meio dos quais indivíduos e organizações, no âmbito de uma determinada área de atuação, perseguiriam seus interesses próprios. Deste modo, a governança expressaria um sistema de ordenação fundado tanto em relações interpessoais como em regras e em sanções explícitas, motivo pelo qual, enquanto sistema de ordenação, implicaria a aceitação da maioria (ou pelo menos dos atores mais poderosos) para poder funcionar ao passo que os governos poderiam, em tese, funcionar mesmo diante de uma forte oposição". VILLAS BOAS FILHO, Orlando. A governança em suas múltiplas formas de expressão: o delineamento conceitual de um fenômeno complexo. **Revista estudos institucionais**, vol. 2, n. 2, 2016, pp. 673-698. p. 677

[264] "Dessa forma, tendo em vista que a internet é um fenômeno que abarca fronteiras transnacionais, a questão da regulação da internet é importante uma vez que se buscará estabelecer normas e princípios mínimos que protejam os direitos à privacidade em âmbito mundial". DIAS, P. Y. Regulação da internet como administração da privacidade. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 9, n. 1, p. 167-182, maio de 2017. p. 168

[265] "Borders have a legal impact, and the reach of law across any border often becomes a matter of great controversy. Even in an era of instant global communication, geography continues to play a major role". BIEGEL, Stuart. **Beyond our control?** Confronting the limits of our legal system in the age of cyberspace. Cambridge: MIT, 2001. p. 111

tarefa de adotar parâmetros mínimos de proteção destes dados e da privacidade? Há quem defenda, ainda, deixar a responsabilidade na mão das próprias pessoas[266], de forma que estas encontrem maneiras de se proteger neste cenário, ou quem defenda a regulação por *design*[267], imprimindo parâmetros regulatórios na própria arquitetura lógica e física da internet.

Postula-se, todavia, e visando a maior proteção possível da privacidade, da liberdade e dos aspectos da dignidade nela subentendidos, que o vigor da imposição normativa emanada pela regulação estatal – porque, sim, defende-se veementemente a presença do Estado neste cenário – deve ser extremamente intenso, sobretudo ante aos interesses concorrentes no contexto da monetização de dados pessoais e pela necessidade[268] de proteção do direito fundamental à privacidade.

Necessário esclarecer, neste ponto, a distinção que certos teóricos fazem ao tratar do tema de regulação e governança da internet: costumam dividi-la em "cestas"[269], entendidas assim como campos, searas distintas de uma mesma conjuntura. Assim, há a cesta jurídica, a cesta econômica, a cesta de infraestrutura, cesta sociológica, etc. Este trabalho trata, de acordo com esta nomenclatura, da "cesta jurídica"[270], ainda que simpatizemos, como se verá adiante, com o trabalho de Lawrence Lessig e o seu "*code is law*" (código é lei, em tradução livre – código aqui entendido como sendo o informático); argumenta-se, adiante, como o Estado pode dispor suas normativas e institutos para

---

[266] Por exemplo, Bruno Bioni, ao tratar da proteção de dados pessoais no contexto das cidades inteligentes: "Essa é justamente uma abordagem que articula a tecnologia como um elemento de capacitação e de transparência para que o cidadão controle seus dados e sobre o que deles é extraído para a gestão da cidade. O resultado esperado é que haja um arranjo de 'governança coletivo', em que cada um dos cidadãos contribua para um 'controle democrático' da arquitetura informacional da cidade". BIONI, op. cit., p. 58

[267] "Data protection through system design refers to a level preceding regulation of the steps of data processing. In summarizing broad discussions, it can be described as 'data protection functionality incorporated into systems and procedures'. […] It has a broad scope: from the shaping of administrative competences to which data processing operations are oriented, to organizational and procedural approaches, to the technical setup of data processing equipment. Understood in this way, data protection through system design is an evidently ambitious task to fulfill" ALBERS, op. cit., p. 230

[268] "Já em relação à proteção de direitos fundamentais, o contexto atual de avanços das tecnologias digitais em rede deu nova dimensão à necessidade de proteção de algumas garantias e preceitos constitucionais, como o direito à liberdade de expressão (em suas dimensões coletiva e individual), os direitos à privacidade e intimidade e até a proteção de menores". BAPTISTA, Patrícia; KELLER, Clara Iglesias. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. **RDA – Revista de Direito Administrativo**, Rio de Janeiro, v. 273, p. 123-163, set./dez. 2016. p. 141

[269] Conferir: KURBALIJA, Jovan. **Uma introdução à governança da internet**. Trad.: Carolina Carvalho. São Paulo: Comitê Gestor da Internet no Brasil, 2016.

[270] Ou em termos de 'relação de normatização' existente entre tecnologia e regulação, como querem Baptista e Keller: "Por fim, a relação de normatização entre regulação e tecnologia é aquela em que a tecnologia figura como objeto da regulação, pelo exercício do poder regulador propriamente dito, especialmente por meio de suas competências normativas. É a conformação da tecnologia à lógica principiológica que baseia a regulação setorial em geral, e pode ser exercida por diferentes mecanismos de intervenção. Apesar da dificuldade de definição do que vem a ser efetivamente regulação da tecnologia (diante da diversidade de abordagens sobre cada um dos termos que compõem o conceito), a professora australiana Bennett Moses (2013) entende que, em última análise, a regulação da tecnologia é o instrumento por meio do qual o direito deve estender sua influência sobre o novo ambiente tecnológico […]". BAPTISTA; KELLER, op. cit., p. 137

regular o atual cenário de monetização de dados pessoais de forma que o direito à privacidade seja protegido[271] tanto quanto o possível.

Neste panorama, a regulação do risco, atribuindo a característica de metal radioativo ao uso dos dados pessoais, aparenta ser ferramenta que traduz uma força mínima neste sentido: de um lado, pois revitaliza a capacidade normativa e sancionatória do Estado nacional, que padece de força ante a globalização e seus fluxos supranacionais e, de outro, porque impõe aos interessados em manusear os dados pessoais medidas apriorísticas de regulação severas, intensas, construindo instrumentos sancionatórios e responsabilizadores igualmente severos, já que, como se demonstrou, o fruto da contextualização da privacidade no cenário da monetização de dados pessoais, considerada a necessidade de proteção destes dados, exsurge como uma imperiosa e necessária salvaguarda de aspectos da liberdade e da dignidade humana.

Assim, pretende-se, ao final do capítulo, sugerir soluções que, ao mesmo tempo que sejam de cunho geral, abstrato e de forte teor principiológico, consigam ostentar em si a atemporalidade necessária[272] para o trato desta temática. Acredita-se que lançar mão de proposições demasiadamente específicas, técnicas e estreitas, além de ser tarefa hercúlea, densa e que escapa ao objetivo desta dissertação, porá em risco de veloz obsolescência o presente trabalho.

Desta forma, não tentaremos adequar modelos pré-definidos de regulação ao âmbito da monetização de dados pessoais, senão que tomaremos o caminho oposto, partindo das problemáticas e das necessidades que foram consideradas ante a construção teórica proposta; nos limitaremos, ainda, a gizar o cenário nacional regulatório como ponto de partida – até mesmo como norte para a reinserção do Estado no âmbito das redes – apontando ainda os diplomas legais e institutos aptos a atuar nesta conjuntura (como objetos lançadores de sombra).

---

[271] "Ultrapassada a ideia de regulação como remédio reservado estritamente ao mau funcionamento do mercado, é possível legitimar a intervenção regulatória com base em outras justificativas como a promoção de direitos fundamentais e de valores sociais e culturais […]". Ibidem, p. 140

[272] "Of course, regulation questions in this context are made even more complicated by the rapidly changing technological environment. Given the extent of the recent changes and the fact that few people could anticipate the scope of these changes during the past decade, an understanding of how the online world might be further transformed over the next ten to twenty years is essential if appropriate rules and viable governance mechanisms are to be established". BIEGEL, op. cit., p. 47

4.1 O CENÁRIO REGULATÓRIO BRASILEIRO

Na ordem econômica[273] estipulada pelo constituinte de 1988, certos nortes e princípios foram privilegiados, orientando a direção do Estado em relação às dinâmicas econômicas. Dentre eles, a livre iniciativa, a propriedade privada, a livre concorrência e a defesa do consumidor são exemplos, retirados do art. 170 da Constituição Federal.

Assim, a Constituição adotou uma economia de mercado, de natureza capitalista[274], tendo o Estado participação reduzida no âmbito econômico. No protagonismo que lhe coube, a opção política escolhida – notadamente a partir da década de 1990 e das desestatizações – foi a de um Estado regulador, com atuação limitada a setores específicos da economia, considerados de sensível importância para, por exemplo, a soberania nacional (como é o caso da matriz energética do petróleo, traduzida na existência da Petrobras e da Agência Nacional do Petróleo).

Em tal paradigma[275], o Estado, ao mesmo tempo em que primou pela livre atuação, livre concorrência e livre iniciativa econômica dos particulares, também delegou a prestação de determinados serviços públicos à iniciativa privada, reduzindo-se ao papel de agente normativo e regulador da atividade econômica, exercendo funções de fiscalização, incentivo e planejamento, sendo este último determinante para o setor público e meramente indicativo para o setor privado, consoante a intelecção do art. 174 da Constituição.

Desta feita, visando fiscalizar as atividades econômicas com a menor interferência estatal possível, o Brasil consagrou uma abordagem regulatória[276], criando, em determinadas hipóteses,

---

[273] Para o eminente jurista e ex-ministro do STF, Eros Grau, ordem econômica é o "modo de ser empírico de uma determinada economia concreta"; é a "expressão que designa o conjunto de todas as normas (ou regras de conduta), qualquer que seja a sua natureza (jurídica, religiosa, moral), que respeitam à regulação do comportamento dos sujeitos econômicos"; é também "o sistema normativo (no sentido sociológico) da ação econômica"; e é, ainda, "ordem jurídica da economia". GRAU, Eros Roberto. **A ordem econômica na constituição de 1988**. São Paulo: Malheiros, 2006. p. 65

[274] TAVARES, André Ramos. **Direito Constitucional Econômico**. 3 ed. São Paulo: Método, 2011. p. 234

[275] "'Regulação', por sua vez, parece assumir sentido mais amplo do que a 'administração ordenadora' e o 'poder de polícia'. A doutrina do Direito Público Econômico faz uso deste termo para tratar da mecânica estatal de ordenação das atividades econômicas em geral, incluindo, portanto, os serviços públicos e as atividades econômicas em sentido estrito. Sendo assim, o Estado desempenha a regulação tanto quando tem vínculo genérico com o administrado (livre iniciativa da atividade econômica em sentido estrito) quanto no caso de possuir vínculo específico (serviços públicos prestados mediante concessão ou permissão)". ARAGÃO, Alexandre Santos de. **Agências Reguladoras e a evolução do Direito Administrativo Econômico**. 3ª ed. Rio de Janeiro: Forense, 2013. p. 37

[276] "podemos condensadamente definir a regulação estatal da economia como o conjunto de medidas legislativas, administrativas, convencionais, materiais ou econômicas, abstratas ou concretas, pelas quais o Estado de maneira restritiva da autonomia empresarial ou meramente indutiva, determina, controla ou influencia o comportamento dos agentes econômicos, evitando que lesem os interesses sociais definidos no marco da Constituição e os orientando em direções socialmente desejáveis". Ibidem, p. 40

entidades reguladoras[277] com capacidade para editar normativas, fiscalizar sua aplicação e repreender possíveis violações, a depender do nicho econômico regulado.

Assim, em um cenário de livre iniciativa e Estado regulador, marcado, ainda, por vigorosa e constante evolução tecnológica[278] e forte influência da sociedade em rede e suas problemáticas e desafios, é que foi o Marco Civil da Internet editado, com vistas a acompanhar este desenvolvimento[279].

Esta lei previu, como fundamentos para o uso da internet no País, em seu art. 2º, V, a livre iniciativa, a livre concorrência e a defesa do consumidor, bem como a liberdade dos modelos de negócio promovidos na rede (no art. 3º, VIII) – desde que não conflitantes com os demais princípios do ordenamento jurídico pátrio ou advindos de tratados internacionais. Destarte, os modelos de negócio (que se multiplicam, como se pôde demonstrar, por parte dos prestadores de serviços *online*), no âmbito da internet, devem respeito[280] à proteção dos dados pessoais, consoante o disposto no art. 3º, III, do Marco Civil.

Como introduzido anteriormente, o Decreto nº 8.771/2016 foi sancionado na intenção de preencher certo vácuo normativo demandado pelas disposições do Marco Civil – a proteção aos dados pessoais está prevista como direito, mas não garantido e regulamentado por lei. Com efeito, e coadunando com a função fiscalizatória antevista no art. 174 da Constituição Federal, o Decreto em fito estabeleceu certos parâmetros para fiscalização e apuração de infrações dos procedimentos para guarda e proteção de dados.

Assim, na falta da Autoridade Nacional de Proteção de Dados, vetada da Lei Geral de Proteção de Dados Pessoais, analisaremos as disposições regulatórias presentes no Decreto nº 8.771/2016 e, a partir delas, trabalharemos perspectivas para o cenário nacional de monetização de dados pessoais. Mister ressaltar que a sanção do PLC 53/2018 houvesse sido realizada em seus

---

[277] "Como foi ressaltado, a criação das agências reguladoras está estreitamente relacionada com um duplo movimento: o processo de enxugamento do papel do Estado na economia – ou a reforma de desestatização – e o conjunto de instrumentos de reforma administrativa que visavam à flexibilização da gestão pública" PECI, Alketa. Regulação comparativa: uma (des)construção dos modelos regulatórios. In:_____. (org.). **Regulação no Brasil**: desenho, governança, avaliação. São Paulo: Atlas, 2007. p. 83

[278]"As concepções clássicas do direito administrativo são sempre desafiadas por três vetores: o aumento da consciência do cidadão (vertente política), as realidades ditadas pela dinâmica do mercado (vertente econômica) e a evolução do conhecimento aplicado (vertente tecnológica)". MARQUES NETO, Floriano de Azevedo; FREITAS, Rafael Véras de. Uber, WhatsApp, Netflix: os novos quadrantes da publicatio e da assimetria regulatória. **Revista de Direito Público da Economia – RDPE**, Belo Horizonte, ano 14, n. 56, p. 75-108, out./dez. 2016. p. 75

[279] "O Direito e a tecnologia não existem em um vácuo, separados e independentes entre si. […] Os avanços tecnológicos também tornam obsoletos certos dilemas jurídicos, ao mesmo tempo em que criam inúmeros outros." LEONARDI, Marcel, op. cit., p. 27

[280] "Fato é que os agentes econômicos comportam-se de uma forma crescente, que procura não encontrarem limites. Se porventura os encontrar, visam a os transpor da maneira mais eficaz e com menores custos. Assim, a liberdade econômica tende a ser conduzida a abusos […]. O poder econômico somente se retrai na presença de outro poder privado (igual ou superior), ou diante de um poder público". MOREIRA, Egon Bockmann. Agências reguladoras independentes, poder econômico e sanções administrativas. In: PECI, Alketa (org.). **Regulação no Brasil**: desenho, governança, avaliação. São Paulo: Atlas, 2007. p. 103

integrais termos, com a criação da ANPD, se teria suprido a necessidade de análise do arcabouço legal nacional em busca de nortes reguladores – sendo este ainda outro motivo que influencia na postura deste trabalho, com a produção de postulados abstratos, gerais e atemporais[281], e que carreguem em sua natureza, desta maneira, a capacidade de atuarem efetivamente, independentemente do cenário posto; no caso, com o advento da LGPD, e eventual criação da ANPD, apontamentos legais que continuem úteis e não obsoletos.

Destarte, assente a premência de se regular o cenário sob exame[282], temos que, quando se fala em regulação para situações que envolvem a internet, alguns modelos surgem com mais frequência como possíveis soluções. Sem embargo, três perspectivas regulatórias são sempre mencionadas: a regulação estatal[283], traduzida no protagonismo de entes da Administração na edição de normativas, fiscalização de preceitos e aplicação de sanções, em atuação direcionada a determinado recorte ou segmento de mercado (sendo exemplo disto as agências reguladoras); a auto-regulação[284], que consiste em uma atuação regulatória de protagonismo dos próprios entes regulados, que atuam construindo padrões comuns de qualidade e de atuação, códigos e padronizações, em um cenário de composição e criação de mecanismos próprios de *enforcement*; por fim, modalidade que surge com diferentes nomenclaturas, a co-regulação[285], que consistente na divisão de tarefas e responsabilidades entre autoridades regulatórias e agentes regulados.

Existem críticas e elogios para as três proposituras. Em relação à regulação estritamente estatal, critica-se a centralidade exacerbada, que pode ocasionar a falta de entrada nos setores

---

[281] "Quando a decisão de regular é relativamente contemporânea ao surgimento da nova tecnologia, até mesmo por falta de elementos de informação e dados de desempenho, o regulador não terá como ser detalhista. Nesse caso, será forçado a optar por bases mais principiológicas, parâmetros gerais, sob pena de fracasso no seu desiderato. Ao contrário, se a opção de regular se der em momento posterior, quando a inovação disruptiva já estiver mais consolidada, é provável que o regulador acabe optando por uma regulação mais extensiva e minudente, com foco nas questões surgidas no processo de consolidação". BAPTISTA; KELLER, op. cit., p. 155

[282] "Mais do que a edição de normas específicas sobre proteção de dados pessoais, também se faz necessária a existência de instância regulatória capaz de apresentar opiniões técnicas específicas à proteção da privacidade nos diferentes segmentos de mercado e de realizar controle unificado e homogêneo do cumprimento das disposições sobre proteção de dados pessoais". BRASIL. Ministério da Ciência, Tecnologia Inovações e Comunicações; Ministério do Planejamento, Desenvolvimento e Gestão; Banco Nacional do Desenvolvimento. **Relatório do plano de ação – capítulo regulatório:** Produto 8. Brasília, 2017. p. 26

[283] "em que a organização de determinado segmento de mercado é concentrada e conduzida por órgão da Administração direta ou indireta, como é o exemplo das Agências Reguladoras (Agência Nacional de Energia Elétrica - ANEEL e Agência Nacional de Telecomunicações - ANATEL, por exemplo)". Ibidem, p. 26-27

[284] "Por exemplo, considerando o contexto da regulação da internet como administração da privacidade, percebe-se que é possível que as empresas estabeleçam padrões mínimos que cada entidade precisa seguir para evitar que a privacidade dos cidadãos seja violada. As empresas podem criar manuais de procedimentos de forma que preservem mais as informações pessoais e protejam a privacidade dos seus usuários. De acordo com a teoria responsiva de regulação de Ayres e Braithwaite, esses padrões mínimos seriam a auto-regulação localizada na base da pirâmide, baseada no diálogo, na cooperação e na responsabilidade". DIAS, op. cit., p. 170

[285] Que pode ser chamada também de governança, haja vista o caráter difuso de produção de normas, sua aplicação e fiscalização (vide VILLAS BOAS FILHO, op. cit., p. 677); e pode ser o "balanço entre o mix de direito e tecnologia" estipulado por Lessig, em busca de um equilíbrio entre os interesses públicos e privados (LESSIG, op. cit., p. 20).

regulados, o surgimento de rejeição e mesmo o impedimento da inovação[286]; por outro lado, exsurge como perspectiva apta a realizar uma fiscalização mais eficaz das normativas impostas, promover valores e salvaguardar direitos[287], haja vista o alcance e efetividade do poder sancionador Estatal.

Quanto a auto-regulação, critica-se a falta da natureza cogente[288] das normas acordadas, a possibilidade de criação de monopólios em situações como a em exame, causando situações de vulnerabilidade dos sujeitos de direito[289], que envolvem nichos altamente tecnológicos e especializados, assim como a vulnerabilidade que se encontrarão os consumidores daquele recorte econômico, que dependerão da "boa vontade" dos agentes econômicos em cumprir com suas promessas de auto-regulação[290]; valoriza-se, nesta perspectiva, a dinamicidade, celeridade e desburocratização para a constituição e aplicação das soluções acordadas[291].

Dentre as hipóteses levantadas, a que recebe mais elogios do que críticas é a co-regulação. Há quem diga que esta possibilidade, por incluir a participação dos agentes regulados na tomada de decisões, possa ensejar a captura da autoridade ou agência regulatória pelos interesses econômicos

---

[286] "Em muitos casos, a sobrecarga da política regulatória com a promoção de muitos objetivos simultaneamente pode ter o efeito de impedir a inovação. E a garantia da inovação, como apontam os estudiosos, deve ser tida como o objetivo central das intervenções regulatórias em face das tecnologias". BAPTISTA; KELLER, op. cit., p. 151

[287] "À postura cautelosa se opõe outra, mais ativa, e que justifica a intervenção regulatória em novas tecnologias igualmente com a finalidade de promover uma gama bastante ampla de objetivos e interesses sociais, que vão desde a proteção de minorias, do meio ambiente, até a cultura e da língua nacionais e a promoção do desenvolvimento". Ibidem, p. 151

[288] "De todo modo, não se considera que a auto-regulação seria suficiente para devidamente normatizar e fiscalizar o respeito à privacidade na Internet, especialmente no médio e longo prazo. Isso porque experiências de auto-regulação muitas vezes não são multissetoriais ("*multistakeholder")*, dependendo de adesão voluntária dos diversos atores. Ainda, as normas editadas por meio da auto-regulação não são cogentes e o órgão deterá limitadas capacidades sancionatórias". BRASIL. Ministério da Ciência, Tecnologia Inovações e Comunicações; Ministério do Planejamento, Desenvolvimento e Gestão; Banco Nacional do Desenvolvimento. **Relatório do plano de ação – capítulo regulatório:** Produto 8. Brasília, 2017. p. 39

[289] "Even the authors who consider data processing consent a crucial component of data protection law which gives effect to the goal it purports, admit that the way in which it is currently devised in the law and its application provide an insufficient protection for individuals and an inadequate safeguard for the values it aims to protect vis-à-vis the realities of marketplace practices and economic interests. […] a large range of extra-legal factors undermines the privacy interests that consent mechanisms are supposed to promote or embody, as the degree of choice presupposed by these mechanisms will not often be present for certain services or products, particularly offered by data controllers in a monopoly or near-monopoly position". ZANFIR, Gabriela. Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. In: GUTWIRTH, Serge, et al (eds.). **Reloading Data Protection**: Multidisciplinary Insights and Contemporary Challenges. Dordrecht (Holanda): Springer, 2014. pp. 237-258. p. 239

[290] "A principal crítica à abordagem dos EUA [que adota a autorregulação] é que as pessoas são colocadas em uma posição relativamente vulnerável, uma vez que raramente sabem da importância das opções oferecidas pelas políticas de privacidade e geralmente concordam com tais políticas sem se informarem a seu respeito". KURBALIJA, op. cit., p. 142

[291] "Papel indiscutivelmente relevante na disciplina das inovações disruptivas pode ser reservado aos mecanismos de autorregulação. Como na função atribuída à Google no resguardo do direito ao esquecimento narrado no início deste trabalho, multiplicam-se os exemplos de instrumentos de autorregulação e/ou regulação compartilhada na disciplina das plataformas digitais, redes etc. Muitas dessas plataformas, por exemplo, estabelecem rotinas de rigoroso controle de qualidade, em geral com o auxílio dos seus próprios usuários, constantemente estimulados a avaliar os serviços usufruídos". BAPTISTA; KELLER, op. cit., p. 156

envolvidos; não nos delongaremos neste ponto, mesmo sabendo que trata-se de hipótese inteiramente plausível[292].

O que importa para o presente trabalho – e isto é o ponto forte desta perspectiva regulatória – é a capacidade de maximização do alcance regulador proporcionada pela união de forças entre regulador e regulados. A junção do expertise técnico, com inserções do terceiro setor, da academia, de jurisconsultos e representantes governamentais tornam não apenas mais completo o arcabouço justificador da regulação, como também melhor equipam o arsenal para pô-la em prática.

O Brasil, inclusive, vem adotando esta perspectiva em matéria de internet, tendo homenageado no Marco Civil da Internet[293] o Comitê Gestor da Internet no Brasil (CGI.br), órgão multiparticipativo e de caráter orientador, como entidade "conselheira" em termos de internet, além de ter proposto, no PLC 53/2018, a criação do Conselho Nacional de Proteção de Dados Pessoais, entidade que contaria com um colegiado multissetorial – mas que foi vetada pela sanção presidencial quando da edição da LGPD.

Independentemente do modelo a ser escolhido pelo Brasil (que foi definido a partir do veto sobre a Lei Geral de Proteção de Dados[294]), defende-se, basicamente, dois postulados: primeiro, que a presença do Estado é essencial neste cenário, devendo atuar na regulação da monetização de dados pessoais (afastando, assim, a possibilidade da autorregulação como uma opção isolada) por meio de um ente regulador próprio[295]; e, segundo, que o desiderato último, a qual se presta todos os meios possíveis, é a proteção da privacidade e valores conexos dos titulares dos dados pessoais (informando condicionantes aos modelos de regulação estatal e co-regulação).

---

[292] JORDÃO, Eduardo. RIBEIRO, Maurício Portugal. Como desestruturar uma agência reguladora em passos simples. **Revista Estudos Institucionais**, Vol. 3, 1, 2017, pp. 182-205.

[293] Art. 24, II, do MCI: "Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil: […] II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil".

[294] Vozes da academia já levantaram-se contra avanços por parte do chefe do executivo em retirar da LGPD a existência da ANPD: "Como disse acima, a LGPD vai agora para sanção presidencial. Temer pode acatar a lei como um todo, negá-la completamente ou vetar determinadas partes. Muito se discute sobre a possibilidade de veto do trecho que cria a Autoridade Nacional de Proteção de Dados, com base em uma série de argumentos, tanto jurídicos, políticos e orçamentários. Todavia, a entrada em vigor de uma lei geral de proteção de dados sem uma autoridade autônoma e independente pode ter um impacto indesejado em sua eficácia. Pode até mesmo tornar a lei incompleta, uma vez que o seu texto faz menção à autoridade 56 vezes, e determinada partes simplesmente não farão sentido sem a sua existência. Por isso, é importante que a existência desse novo órgão seja garantida". MONTEIRO, Renato Leite. **Presidente Temer, a lei de dados precisa de seu órgão fiscalizador**. Disponível em: <https://brasil.elpais.com/brasil/2018/07/13/opinion/1531506142_357368.html>. Acesso em: 24 jul. 2018.

[295] "Em geral, mas com alguma divergência, considera-se que deverá haver autoridade única, centralizada, permeável à participação de atores relevantes, composta por corpo técnico especializado e dotada de independência financeira e decisória". BRASIL. Ministério da Ciência, Tecnologia Inovações e Comunicações; Ministério do Planejamento, Desenvolvimento e Gestão; Banco Nacional do Desenvolvimento. **Relatório do plano de ação – capítulo regulatório:** Produto 8. Brasília, 2017. p. 38

É essencial a presença do Estado[296], como já vem se defendendo, em razão dos riscos que esta atividade ostenta para os direitos fundamentais dos sujeitos de direito. Os dados não são o "novo óleo"; conforme argumentamos, os dados são o novo urânio, precisamente em virtude dos riscos que ostenta. Nesse cenário é que se percebe, uma vez mais, a precisão de uma agência regulatória, capaz de fazer valer as normas que visam proteger os direitos dos titulares dos dados pessoais, editando normativas de efeito vinculante, fiscalizando tais atividades e aplicando, quando necessário, sanções adequadas às eventuais violações.

Destarte, ante a inexistência de ente específico, já que, como repetidamente afirmado, a LGPD foi sancionada sem a criação da ANPD, analisaremos o arcabouço legal existente em busca de saídas para este imbróglio; tal esforço não se mostra inútil por duas razões – primeiro, porque buscará atribuir competências regulatórias aos entes mencionados pelas leis existentes na ausência da ANPD; e, segundo, caso seja criada a ANPD por meio de projeto de iniciativa do Executivo[297], servirá como solução subsidiária durante o período previsto de *vacatio legis* de 18 meses após a sua publicação (conforme art. 65 da LGPD).

Assim, de posse do resultado desta análise, sugeriremos os apontamentos legais que consideramos necessários à salvaguarda do direito fundamental à privacidade na conjuntura em tela.

4.2 DIPLOMAS LEGAIS NACIONAIS E SEUS CONTORNOS REGULATÓRIOS

Primeiramente, antes de adentrar sobre o tema da regulação, importa esclarecer que o objeto desta regulação, a "monetização de dados pessoais", será tomado como um conceito guarda-chuva apto a englobar as várias hipóteses de uso com fins econômicos dos dados pessoais.

No Marco Civil da Internet e no Decreto nº 8.771/2016, encontramos as expressões endereço de protocolo de internet (endereço IP)[298], registro de conexão[299], registro de acesso a aplicações de internet[300], dados cadastrais[301], dado pessoal[302] e tratamento de dados pessoais[303].

---

[296] "The answer is not in the knee-jerk antigovernment rhetoric of a libertarian past: Governments are necessary to protect liberty, even if they are also able to destroy it". LESSIG, op. cit., p. xv

[297] Este foi, inclusive, o argumento central para o veto a criação da ANPD – que existiria vício de iniciativa na sua constituição, já que originária das Casas Legislativas.

[298] "Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção: III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais".

[299] "Art. 4º […] VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados".

[300] "Art. 4º […] VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP".

[301] "Art. 11 […]; § 2º São considerados dados cadastrais: I - a filiação; II - o endereço; e III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário".

Destarte, como dados pessoais, tomaremos por espécie não apenas aqueles que se inferem diretamente do seu conceito no art. 14, I, do Decreto nº 8.771/2016 e do art. 5º, I, da LGPD, mas, também o endereço IP, o registro de conexão e de acesso a aplicações, assim como os dados cadastrais, posto que encaixam-se na definição de dado pessoal – são relacionados, invariavelmente, a pessoa natural identificada ou identificável.

A monetização de dados pessoais, por sua vez, não pode ser tratada como sinônimo de tratamento de dados pessoais em razão de esta última expressão ser mais abrangente que a primeira: ela engloba, por exemplo, o tratamento de dados pessoais por entidades públicas e organizações não governamentais, que não possuem, *a priori*, finalidade econômica nesta atividade.

Portanto, entendemos que monetização de dados pessoais é espécie do gênero tratamento de dados, previsto no art. 14, II, do Decreto nº 8.771/2016 e no art. 5º, X, da LGPD, e designa aquelas operações realizadas com dados pessoais que possuem finalidade de monetização, estando excluídas, portanto, as situações que envolverem entes públicos e outros órgãos sem fins lucrativos.

Adiante, partiremos de uma análise do MCI e do seu decreto regulador para extrair orientações acerca da regulação da monetização de dados pessoais, sobretudo em termos de competência frente a ausência de uma autoridade única.

4.2.1 O Marco Civil da Internet (Lei nº 12.965/2014) e seu Decreto regulador (nº 8.771/2016)

O Marco Civil da Internet, lei de caráter substancialmente axiológico[304], estabelece diretrizes básicas para o uso da internet no País, bem como princípios informadores das relações *online* e direitos dos internautas. Dentre suas disposições, consta a garantia ao direito à privacidade e intimidade, considerada, ao lado da liberdade de expressão, condição *sine qua non* "para o pleno exercício do direito de acesso à internet" (art. 8º).

Como já debatido, o direito à privacidade é um direito fundamental do cidadão, previsto no artigo 5º da CF/88, em seus incisos X e XII[305], possuindo proteção e garantia constitucional.

[302] "Art. 14. Para os fins do disposto neste Decreto, considera-se: I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa".

[303] "Art. 14 […] II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

[304] "O Marco Civil da Internet é uma legislação baseada em princípios. Foi propositalmente concebida para esse fim: definir os valores básicos que a sociedade pretende proteger no uso da internet no Brasil." ZANATTA, Rafael A. F. A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet, in: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. **Direito e Internet III**: Marco Civil da Internet. São Paulo: Quartier Latin, 2015, p. 447-470. p. 462

[305] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade,

Reforçado através da previsão expressa no artigo 7º do Marco Civil da Internet[306], em seus três primeiros incisos, é notável a preocupação do legislador em salvaguardar e garantir este direito dos usuários na rede, evitando possíveis violações[307].

Apesar destas disposições, o Marco Civil necessitou[308] de regulamentação em determinadas temáticas. Neste ensejo, editou-se o Decreto nº 8.771/2016, que trata das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

O Decreto, sancionado pela então presidente Dilma Rousseff em 11 de maio de 2016[309] – ressalte-se que ela foi afastada da presidência aos 12 de maio do mesmo ano, quando da abertura do processo de *impeachment* pelo senado – possui alguns méritos[310], como o de definir o conceito de dado pessoal, no art. 14, I, e o tratamento de dados pessoais, no inciso II do mesmo dispositivo.

Esta pressa em sancioná-lo talvez tenha sido a razão das dúvidas advindas da leitura dos arts. 17 a 21. Estes artigos, presentes no Capítulo IV do Decreto em questão, tratam da fiscalização e da transparência em relação às atividades regulamentadas por tal diploma: quais sejam, a degradação de pacotes de dados e a guarda e proteção de dados por provedores (de conexão ou de serviço).

Assim, o art. 17 do Decreto nº 8.771/2016 prevê que a "Anatel atuará na regulação, na fiscalização e na apuração de infrações, nos termos da Lei nº 9.472, de 16 de julho de 1997"; o art.

nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

[306] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.

[307] "Outro problema de importância reside no fato de que o uso das novas tecnologias pode muitas vezes ultrapassar as fronteiras entre o público e o privado a ponto de provocar prejuízos a direitos fundamentais. Como exemplo, podemos citar o emprego de ferramentas de controle e de vigilância na promoção da segurança pública dos Estado como também na prevenção de atos terroristas". RUARO, Regina Linden. **Privacidade e Autodeterminação Informativa:** obstáculos ao Estado de Vigilância? Arquivo Jurídico, Teresina/PI, v. 2, n. 1, jan./jun. de 2015, p. 41-60. p. 42

[308] "É ilusório pensar que a solução para os vários problemas jurídicos do uso da internet está na Lei 12.965/2014. A proteção de dados pessoais, por exemplo, está apenas definida como direito. Não há, por enquanto, garantia suficiente para uma adequada tutela dos dados pessoais no Brasil.". ZANATTA, Rafael A. F., op. cit., p. 462

[309] SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco Civil da Internet**: construção e aplicação. Juiz de Fora: Editar, 2016. p. 29

[310] "Um ponto de grande relevância trazido com Decreto nº 8.771/16 diz respeito a um conceito para a expressão "dados pessoais". Segundo a norma, o dado é uma informação relacionada 'à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa'". PASSOS, Bruno Ricardo dos Santos. **O direito à privacidade e a proteção aos dados pessoais na sociedade da informação:** uma abordagem acerca de um novo direito fundamental. Dissertação (Mestrado – Faculdade de Direito) – Universidade Federal da Bahia. Salvador, 2017. 102 f. p. 95

18, que a "Secretaria Nacional do Consumidor atuará na fiscalização e na apuração de infrações, nos termos da Lei nº 8.078, de 11 de setembro de 1990"; já o art. 19 estipula que a "apuração de infrações à ordem econômica ficará a cargo do Sistema Brasileiro de Defesa da Concorrência, nos termos da Lei nº 12.529, de 30 de novembro de 2011".

O art. 20, por sua vez, determina que os órgãos e as entidades da administração pública federal com competências específicas quanto aos assuntos relacionados a este Decreto atuarão de forma colaborativa, consideradas as diretrizes do CGI.br, e que deverão zelar pelo cumprimento da legislação brasileira, inclusive quanto à aplicação das sanções cabíveis, mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, nos termos do art. 11 do Marco Civil.

Por fim, o art. 21 prevê que a apuração de infrações ao Marco Civil e ao Decreto atenderá aos procedimentos internos de cada um dos órgãos fiscalizatórios e poderá ser iniciada de ofício ou mediante requerimento de qualquer interessado.

Como se vê, o legislador não foi expresso em determinar a competência regulatória para as atividades em questão; em vez disto, elencou a ANATEL e a Senacon[311] como entidades aptas a atuar em matéria de regulação, ao mesmo tempo em que citou o Sistema Brasileiro de Defesa da Concorrência, no art. 19, bem como órgãos e outras "entidades da administração pública federal com competências específicas quanto aos assuntos relacionados a este Decreto", no art. 20. Este último dispositivo é demasiado enigmático quanto à distribuição das competências que o Decreto nº 8.771/2016 prevê no tocante a monetização dos dados pessoais.

A seguir, o trabalho desenvolveu-se no intuito de afastar as dúvidas quanto às competências previstas no Decreto sob exame, analisando, para tanto, as disposições acima apontadas.

4.2.2 Competência para regular em matéria de dados pessoais de acordo com as disposições do Decreto nº 8.771/2016

Já se adiantou, em momento anterior, as disposições dos artigos que tratam da fiscalização e transparência neste decreto.

Isto posto, podemos inferir que o Decreto conferiu: competência para regular, fiscalizar e apurar infrações à Anatel, nos termos da lei que a criou (Lei nº 9.472/1997); competência para fiscalizar e apurar infrações à Senacon, nos termos do Código de Defesa do Consumidor; e, para

[311]A Secretaria Nacional do Consumidor - Senacon, criada pelo Decreto nº 7.738, de 28 de maio de 2012, compõe a estrutura do Ministério da Justiça e tem suas atribuições estabelecidas no art. 106 do Código de Defesa do Consumidor e no art. 3º do Decreto nº 2.181/97. A atuação da Senacon concentra-se no planejamento, elaboração, coordenação e execução da Política Nacional das Relações de Consumo, tendo por objetivos garantir a proteção e exercício dos direitos dos consumidores, a promoção da harmonização nas relações de consumo e incentivo na integração e na atuação conjunta dos membros do Sistema Nacional de Defesa do Consumidor – SNDC.

apurar infrações à ordem econômica, competência ao Sistema Brasileiro de Defesa da Concorrência – SBDC, nos termos da Lei nº 12.529/2011.

Previu, ainda, que os órgãos e as entidades da administração pública federal com competências específicas quanto aos assuntos relacionados a este Decreto deverão atuar de forma colaborativa, consideradas as diretrizes do CGI.br (Comitê Gestor da Internet no Brasil), consoante o art. 20.

A previsão mais problemática, entretanto, se infere do art. 21, afirmando o legislador que a apuração de infrações ao Marco Civil da Internet e ao Decreto nº 8.771/2016 deverá atender aos procedimentos internos de cada um dos órgãos fiscalizatórios, podendo ser iniciada de ofício ou mediante requerimento de qualquer interessado. Tão ampla e abrangente determinação acaba por minar a certeza jurídica que o diploma legal deveria conferir, ao não delimitar com mais especificidade as competências atribuídas.

Delimitemos, pois, de maneira a orientar esta análise, as atividades que serão o escopo da regulação em fito: o Decreto nº 8.771/2016 trata das atividades que envolvam discriminação de pacote de dados, degradação de tráfego de dados e da guarda e proteção de dados. Para este trabalho, importam as atividades relacionadas à guarda e proteção de dados, pois que relacionadas ao tratamento de dados e, portanto, à sua monetização.

Os arts. 13 a 16 do mesmo Decreto são os que abordam tais atividades. O art. 13 prevê que os provedores – tanto de conexão como de aplicações[312] – devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar certas diretrizes sobre padrões de segurança.

O art. 14 define dado pessoal e tratamento de dados pessoais; o art. 15 preleciona, fazendo menção ao art. 11[313] do Marco Civil, a necessidade de estruturação e interoperabilidade dos dados que passem por coleta, armazenamento, guarda ou tratamento em território nacional, para facilitar seu acesso caso sejam alvo de decisão judicial que lhes solicite. O art. 16, por fim, determina o

[312]Provedores de conexão (da intelecção do art. 9º do Marco Civil da Internet) são aqueles que provêem conexão à Internet, que fornecem o fluxo de dados que permitem o acesso à rede mundial de computadores; são provedores de conexão, por exemplo, a NET e a GVT; TIM, Claro e Vivo são exemplos de provedores para dispositivos móveis. Já os provedores de aplicação são conceituados no art. 5º, VII, do Marco Civil da Internet como um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; exemplo deles são o Google, o Facebook, Outlook, Twitter, entre tantos outros dos incontáveis serviços oferecidos online.

[313]Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 19 out. 2017.

dever de clareza e acessibilidade, para com qualquer interessado, sobre os padrões de segurança adotados para proteger os dados pessoais.

Ante o exposto, pode-se ensaiar uma distribuição de competências.

4.2.2.1 Competência da Agência Nacional de Telecomunicações (Anatel)

Primeiramente, analisemos o art. 17 e o papel da Anatel. Pela disposição da Lei nº 9.472/1997, esta autarquia é competente para regular sobre a organização dos serviços de telecomunicações – que inclui, entre outros aspectos, o disciplinamento e a fiscalização da execução, comercialização e uso dos serviços, bem como a implantação e funcionamento de redes de telecomunicações.

É possível delimitar, em um primeiro momento (considerando o uso dos dados pessoais como elaborados nos capítulos anteriores), a atuação da Anatel apenas às atividades relacionadas à discriminação de dados e diminuição de tráfego, pois que diretamente ligadas[314] à competência desta autarquia, nos termos dos arts. 3 a 10 do Decreto nº 8.771/2016. Nesta linha de raciocínio, as atribuições[315] da Anatel se restringiriam às atividades relacionadas à tais práticas[316], como a regulação da velocidade de conexão, a derrubada de sinal, fiscalização dos pacotes de dados, entre outros.

Por outro lado, o art. 3º, IX, da lei que criou a Anatel também prevê como direito dos usuários dos serviços de telecomunicações "o respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço". Retornando ao art. 13 do Decreto nº 8.771/2016, observa-se que os provedores de conexão – agentes econômicos, portanto, regulados pela Anatel – caso guardem, armazenem ou tratem dados pessoais, também devem obediência aos comandos do referido dispositivo e, por conseguinte, ao Decreto.

Importante destacar, para o debate em fito, a Resolução nº 632, de 7 de março de 2014, da Anatel. Esta resolução impõe aos entes regulados a obrigatoriedade de observância ao Regulamento

[314]Art. 3°: O usuário de serviços de telecomunicações tem direito: III - de não ser discriminado quanto às condições de acesso e fruição do serviço.

[315]Neste sentido, a Resolução nº 575, de 28 de outubro de 2011, que trata do regulamento de Gestão da Qualidade da Prestação do Serviço Móvel Pessoal; a Resolução n° 614/2013, que regulamenta o Serviço de Comunicação Multimídia; e a Resolução nº 632/2014, que regulamento os Direitos do Consumidor de Serviços de Telecomunicações.

[316]Concernentes à Instalação, Mudança de endereço, Entrega do documento de cobrança, Atraso na cobrança, Atraso no pagamento da conta, Cobrança indevida e contestação de valores, Interrupção do serviço, Equipamentos, Extinção ou alteração do Plano de Serviço, Ofertas Conjuntas e Promoções, Suspensão do serviço por falta de pagamento, Suspensão a pedido do consumidor e Cancelamento, Fidelização e Velocidade de conexão, por exemplo.

Geral de Direitos do Consumidor de Serviços de Telecomunicações, elencado no Anexo I da apontada resolução. Prevê, em seu art. 3º, VII, regra similar[317] ao art. 3º, IX, da Lei nº 9.472/97.

É de se indagar: receberia mais esta competência regulatória a Anatel, editando atos e normativas sobre tais atividades, ou os entes regulados por ela estariam sujeitos às determinações de um outro órgão regulador? Avancemos na análise dos demais artigos (18, 19, 20 e 21) do Decreto perscrutado, guardando tal questionamento para momento posterior.

4.2.2.2 Competência da Secretaria Nacional do Consumidor (Senacon)

O art. 18 conferiu à Secretaria Nacional do Consumidor capacidade fiscalizatória e de apuração de infrações, consoante o disposto no Código de Defesa do Consumidor. Aqui, cabe fazer menção a posicionamento doutrinário que aponta o microssistema consumerista como um importante bastião, na falta de lei específica[318], para a proteção dos dados pessoais no âmbito da internet.

Os professores Danilo Doneda e Laura Schertel, conforme já mencionado, defendem com maior eloquência o pioneirismo e importância do CDC na proteção dos dados pessoais[319]. Apontam que, apesar da falta de lei específica que aborde de maneira geral e abrangente a proteção dos dados

[317] "Art. 3º O Consumidor dos serviços abrangidos por este Regulamento tem direito, sem prejuízo do disposto na legislação aplicável e nos regulamentos específicos de cada serviço: VII - à privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela Prestadora". AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resolução nº 632, de 7 de março de 2014**. Aprova o Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações – RGC. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/2014/750-resolucao-632>. Acesso em: 30 out. 2017.

[318] "Quais normas jurídicas regulam a proteção de dados pessoais no Brasil? A ideia de "colcha de retalhos jurídica" serve para entender, em primeiro passo, o que já existe no Brasil em termos de proteção de dados pessoais. Seria muita ingenuidade dizer que não há algum tipo de proteção de dados pessoais no Brasil. Antes mesmo da aprovação da Lei 12.965/2014, já existiam normas jurídicas e regulações setoriais para proteção de dados. O problema é que tais normas são fragmentadas e não tratam do direito à proteção de dados pessoais de forma explícita" ZANATTA, op. cit., p. 451

[319] "data protection, in a modern sense, initially emerged in Brazil as a consumer protection issue. In fact, the Consumer Protection Code (Law 8.078 of 1990) provided a multifaceted framework in which privacy and data protection demands could develop and be addressed. As the evolution of the issue in other countries reveals, the right to data protection tends to emerge in those legal fields that are more likely to welcome the new social demands. This task fell in Brazil to the Consumer Protection Code, since it entails a variety of principlebased norms, which are broad enough to offer solutions to new conflicts related to information technology". DONEDA; MENDES; In: GUTWIRTH, et al (eds.), 2014. op. cit., p. 6

pessoais, o CDC traz, mormente as disposições do seu art. 43[320], fundamentos importantes nesta seara.

É importante, ainda, quando se considera que a maioria das relações entre usuários e provedores de aplicações (por exemplo, usuários e *Facebook, Twitter, Google, WhatsApp*, etc) se dão através de contratos de adesão, com termos determinados unilateralmente pelo provedor. Tais contratos estão definidos pelo art. 54 do CDC. Configuram, portanto, relações de consumo e, assim sendo, são merecedoras da proteção por parte deste diploma legal.

Apesar de possuir disposições protetivas dos dados pessoais e contar com mais de 600 entidades públicas em nível federal, estadual e local, proporcionando ao consumidor brasileiro acesso a um considerável número de meios resolutivos de conflitos (como o PROCON e os Juizados Especiais), o Sistema de Proteção ao Consumidor enfrenta o desafio de sustentar as normas já existentes[321]: malgrado possuir certo poder de coerção (aplicar multas e outros tipos de sanções), o aludido sistema carece de ente centralizador, como uma agência de cunho regulatório, que edite atos e normativas vinculantes aos entes submetidos à sua competência, capaz de fiscalizar o cumprimento de suas determinações e de aplicar sanções em face de possíveis violações, não possuindo, de igual maneira, o expertise técnico necessário para tratar das complexas questões inerentes ao cenário de monetização de dados pessoais.

Outro empecilho que limita a abrangência do microssistema consumerista na proteção dos dados pessoais tem relação com os chamados *cookies*[322]. Os *cookies* são gerados pela simples visita de um usuário a um *site* na internet, mesmo que ele não utilize nenhum serviço dali ou faça alguma compra. Assim, há, possivelmente, a preocupação com os dados pessoais e a privacidade, pois os *cookies* permitem certo grau de monitoramento[323] sobre o visitante – que, ressalte-se, nada comprou

[320] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. §1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. §2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. §3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. §4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. §5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. §6º Todas as informações de que trata o **caput** deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

[321] DONEDA, Danilo; MENDES, Laura Schertel., op. cit., p. 13-14.

[322] "A maioria dos sites, hoje, usa cookies para armazenar informações sobre o usuário e sobre a utilização do site em seu computador pessoal. Esses cookies podem armazenar uma variedade de informações e o usuário mantém pouco ou nenhum controle sobre os tipos de dados retidos". CHERRY, Denny, op. cit., p. 7

[323] Assim Daniel J. Solove os define, apontando-os, ainda, como uma forma de "marcador de gado de alta tecnologia": "A cookie is a small text file of codes that is deployed into the user's computer when she downloads a web page. Websites place a unique identification code into the cookie, and the cookie is saved on the user's hard drive. When the user visits the site again, the site looks for its cookie, recognizes the user, and locates the information it collected about

ou contratou e, assim, não adentra no conceito de consumidor propriamente dito. É uma situação, pois, que o corpo legal consumerista aparentemente não alcança[324], mas que necessita de atenção, proteção e regulamentação.

Desta maneira, não é possível pensar a delegação de competência regulatória em matéria de monetização de dados pessoais unicamente à Senacon, principalmente pela limitação de suas atribuições, elencadas no art. 106[325] do CDC. Fazê-lo, ademais, seria sobrecarregar um canal que já se encontra eivado de dificuldades e notória morosidade.

Isso não significa, todavia, que as disposições do CDC e ferramentas da Senacon não confiram certa proteção aos dados pessoais dos consumidores: como se demonstrou, tais institutos possuem ferramental válido para tanto, tutelando tais dados (v. g., as disposições dos incisos II, III, IV, VIII e IX do já mencionado art. 106, CDC) – sobretudo ante a falta de lei específica; o que se quer dizer é que, na perspectiva regulatória anteriormente abordada, que conte com uma agência reguladora com certas competências e atribuições, a Senacon, nos termos do Decreto ora estudado, não é competente (como evidenciam os incisos V, VI e VII do art. 106, CDC – para aplicar sanções, necessita da intervenção da polícia judiciária, MP, e outros órgãos).

4.2.2.3 Competência do Sistema Brasileiro de Defesa da Concorrência (SBDC) e do Comitê Gestor da Internet (CGI.br) e da obscuridade do art. 21 do Decreto nº 8.771/2016

O art. 19, por sua vez, elenca o Sistema Brasileiro de Defesa da Concorrência como apto à apuração de infrações à ordem econômica, nos termos da Lei nº 12.529/2011. É possível descartar o

the user's previous surfing activity in its database. Basically, a cookie works as a form of high-tech cattle-branding." SOLOVE, 2004, op. cit., p. 23-24.

[324] É possível pensar, entretanto, na situação do art. 17 do Código de Defesa do Consumidor, que estabelece a figura do consumidor equiparado. Apesar de, a priori, o simples acessar de um site não entabular relação de consumo, tal fato enseja a utilização de cookies e, portanto, traz em si a potencialidade de devassa de dados pessoais – o que tornaria, em tese, o usuário em consumidor por equiparação. Todavia, é hipótese que não encontra, até o momento, guarida no arcabouço doutrinário nacional.

[325] Art. 106. O Departamento Nacional de Defesa do Consumidor, da Secretaria Nacional de Direito Econômico (MJ), ou órgão federal que venha substituí-lo, é organismo de coordenação da política do Sistema Nacional de Defesa do Consumidor, cabendo-lhe: I - planejar, elaborar, propor, coordenar e executar a política nacional de proteção ao consumidor; II - receber, analisar, avaliar e encaminhar consultas, denúncias ou sugestões apresentadas por entidades representativas ou pessoas jurídicas de direito público ou privado; III - prestar aos consumidores orientação permanente sobre seus direitos e garantias; IV - informar, conscientizar e motivar o consumidor através dos diferentes meios de comunicação; V - solicitar à polícia judiciária a instauração de inquérito policial para a apreciação de delito contra os consumidores, nos termos da legislação vigente; VI - representar ao Ministério Público competente para fins de adoção de medidas processuais no âmbito de suas atribuições; VII - levar ao conhecimento dos órgãos competentes as infrações de ordem administrativa que violarem os interesses difusos, coletivos, ou individuais dos consumidores; VIII - solicitar o concurso de órgãos e entidades da União, Estados, do Distrito Federal e Municípios, bem como auxiliar a fiscalização de preços, abastecimento, quantidade e segurança de bens e serviços; IX - incentivar, inclusive com recursos financeiros e outros programas especiais, a formação de entidades de defesa do consumidor pela população e pelos órgãos públicos estaduais e municipais; XIII - desenvolver outras atividades compatíveis com suas finalidades. Parágrafo único. Para a consecução de seus objetivos, o Departamento Nacional de Defesa do Consumidor poderá solicitar o concurso de órgãos e entidades de notória especialização técnico-científica.

SBDC como competente para regular em termos de dados pessoais, uma vez que se trata de matéria alheia às atribuições[326] de seus órgãos conformadores. Assim, e por tudo que já foi abordado, são hipóteses de atuação do SBDC na temática do Decreto nº 8.771/2016, por exemplo, a fiscalização de violações à neutralidade da rede – seja em detrimento dos consumidores, discriminando-lhes o tráfego, seja pela atuação concorrencial predatória, através de promoções que firam a referida neutralidade.

Do art. 20, pouco se pode aproveitar para o intuito almejado pelo presente trabalho. O legislador expôs, no referido dispositivo, que os órgãos e as entidades da administração pública federal, com competências específicas quanto aos assuntos relacionados a este Decreto, atuarão de forma colaborativa, consideradas as diretrizes do CGI.br. Como se pode perceber, pelo que até agora foi exposto, a especificidade suscitada no art. 20 encontra-se prejudicada pelo laconismo do próprio legislador.

Pode-se inferir, entretanto, duas informações importantes: a primeira, o dever de atuação colaborativa entre os órgãos competentes, homenageando, aparentemente, o modelo de co-regulação; a segunda, a consideração frente as diretrizes do Comitê Gestor da Internet no Brasil. Necessário afirmar, em relação ao CGI.br, que tal órgão não possui competência regulatória[327].

O Comitê Gestor da Internet (CGI.br)[328], originalmente, foi criado com a finalidade de organizar e manter o registro do domínio brasileiro (.br) na rede mundial de computadores. Entretanto, a sua natureza não é a de ente regulatório[329], como se depreende dos diplomas legais que lhe criaram[330] e normatizam; tampouco, entre suas atribuições[331], se encontram capacidades que lhe

---

[326]Atribuições que visam à prevenção e a repressão às infrações contra a ordem econômica, orientada pelos ditames constitucionais de liberdade de iniciativa, livre concorrência, função social da propriedade, defesa dos consumidores e repressão ao abuso do poder econômico.

[327]"A atividade de regulação econômica através da fiscalização não se exaure no definir as condutas (permitidas, proibidas e obrigatórias) e a vistoriar ou supervisionar, mas engloba a capacidade de punir os eventuais desvios. A regulação contempla um amplo conjunto de fenômenos normativos que se sucedem, partindo de um ponto inicial (a Ordem Econômica constitucional) e terminando num estado conclusivo (a aplicação das sanções)". MOREIRA, Egon Bockmann., op. cit., p. 107.

[328]"O Comitê Gestor da Internet no Brasil (CGI.br) foi criado pela Portaria Interministerial nº 147, de 31 de maio de 1995, alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003, para coordenar e integrar todas as iniciativas de serviços da Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Composto por membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica, o CGI.br representa um modelo de governança na Internet pioneiro, no que diz respeito à efetivação da participação da sociedade, nas decisões envolvendo a implantação, administração e uso da rede". BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **CGI.br**. Disponível em: <https://www.governodigital.gov.br/transformacao/cgi-br>. Acesso em: 10 out. 2017.

[329] "autarquias de controle e o poder de 'editar normas gerais sobre o setor sob seu controle'". CARVALHO FILHO, José dos Santos. **Agências reguladoras e poder normativo**. Revista Eletrônica de Direito Administrativo Econômico, Salvador, Instituto Brasileiro de Direito Público, nº 9, fev./mar./abr., 2007. Disponível em: <http://www.direitodoestado.com.br/redae.asp>. Acesso em: 15 de maio de 2017. p. 6

[330] A Portaria Interministerial n° 147, de 31 de maio de 1995, criou o referido órgão; foi complementada em 2003 pelo Decreto nº 4.829, que dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.br, sobre o modelo de governança da Internet no Brasil e que dá outras providências.

confiram poder coercitivo, de fazer valer tanto suas determinações como as leis atinentes, fiscalizar atividades e punir eventuais infrações. Trata-se de um órgão de caráter orientador[332].

Ainda, à obscuridade do art. 20 soma-se a do art. 21[333] do Decreto nº 8.771/2016.

Dele, pode-se retirar que, sendo definida a competência para a apuração de infrações envolvendo os dados pessoais, esta poderá ser iniciada de ofício ou mediante requerimento de qualquer interessado.

Quanto à competência, deverá atender "aos procedimentos internos de cada um dos órgãos fiscalizatórios": é possível teorizar, face a isto, que em termos de guarda e uso (inclusa a monetização) dos dados, a capacidade de apurar infrações dependerá da situação específica na qual os dados em questão foram coletados – e mesmo assim, resta algo de duvidoso.

Por exemplo: caso tenham sido coletados no âmbito de contratos tidos com as operadoras de telefonia móvel (e por ela utilizados), seriam competentes, pelo que foi o exposto, tanto a Anatel (pelas disposições da Lei nº 9.472/97 e da Resolução ANATEL nº 632/2014) como o ferramental do microssistema consumerista[334] (em se tratando de uma relação de consumo); ou, sendo os dados coletados por provedores de aplicativos, agiriam, a depender do caso (como se viu, os *cookies* são exceção, bem como as hipóteses em que há o compartilhamento dos dados pessoais entre empresas[335]), as disposições do Código de Defesa do Consumidor.

Retornemos, agora que analisados os artigos propostos, ao questionamento suscitado no subitem 4.2.2.1. Em retrospecto: caberia à Anatel capacidade regulatória sobre o tratamento de dados pessoais, sobretudo com relação à monetização destes dados, em virtude dos provedores de conexão atuarem neste nicho?

---

[331] Da análise do art. 1º do seu Decreto criador, que estabelece suas atribuições, infere-se que o CGI.br não possui independência e autonomia, pois que composto de membros advindos do meio empresarial; não tem poderes de conciliação, sendo incapaz de mediar conflitos existentes tanto entre consumidores e empresas reguladas, ou mesmo entre entes regulados e o governo; e carece de poderes fiscalizatório e sancionatório, sendo incapaz de impor coercitivamente suas normativas e orientações.

[332] "A partir do comando do Marco Civil, que prestigia a competência do Comitê Gestor da Internet (CGI.br) ao propor diretrizes técnicas para o uso e desenvolvimento da Internet, o Decreto detalha o diálogo regulatório ampliado que deve existir para a melhor regulação e governança da rede no Brasil." SOUZA; LEMOS, op. cit., p. 31

[333] Art. 21. A apuração de infrações à Lei nº 12.965, de 2014, e a este Decreto atenderá aos procedimentos internos de cada um dos órgãos fiscalizatórios e poderá ser iniciada de ofício ou mediante requerimento de qualquer interessado.

[334] E como deixa explícito o parágrafo 2º, art. 1º, da mencionada resolução: "§ 2º A aplicação das regras constantes do presente Regulamento não afasta a incidência da Lei nº 8.078, de 11 de setembro de 1990 – Código de Defesa do Consumidor, do Decreto nº 6.523, de 31 de julho de 2008, e regras complementares dos direitos previstos na legislação e em outros regulamentos expedidos pelas autoridades administrativas competentes." AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resolução nº 632, de 7 de março de 2014**. Aprova o Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações – RGC. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/2014/750-resolucao-632>. Acesso em: 30 out. 2017.

[335] "Tal vulnerabilidade é patente, principalmente se contrastada com outras hipóteses de tratamento de dados pessoais no setor privado, por exemplo, quando ele ocorre em uma relação entre empresas (*business to business*). Essa situação de empresas buscarem dados de outras empresas é bastante comum no mercado, tendo em vista a busca constante pela diminuição de riscos. Nesses casos, naturalmente, trata-se de uma relação civil, entre iguais, e não de uma relação de consumo". MENDES, 2008, op. cit., p. 130

Os elementos até aqui estudados parecem sugerir que a Anatel poderia atuar apenas pontualmente, mas não de maneira central e abrangente, em substituição a uma Autoridade Nacional de Proteção de Dados. Isto porque o próprio art. 17 do Decreto nº 8.771/2016 afirma, expressamente, que a atuação regulatória da Anatel se dará "nos termos da Lei nº 9.472/1997". Esta lei, como foi exposto, lhe confere atribuições que não alcançam o tratamento dos dados pessoais nos parâmetros ora abordados (geral e abrangente).

Além disto, tal delegação de nova competência seria por demais onerosa[336] a esta autarquia, que já possui extenso rol de tarefas[337] em mãos. Todavia, forçoso reconhecer certa lógica ao raciocínio que confere competência para regular esta matéria quando dada no âmbito dos entes regulados pela Agência Nacional de Telecomunicações: é dizer, quando estes entes utilizarem os dados pessoais dos seus usuários (nisto inclusas as práticas de tratamento e monetização dos dados), teria a Anatel capacidade para regular, normatizar, fiscalizar e aplicar sanções em caso de irregularidades.

Importante atentar, ainda que não seja o escopo do presente esforço analítico, que a competência da Anatel para regular nos termos do Decreto nº 8.771/2016 também alcança (senão principalmente) os casos que envolvem a manutenção da neutralidade da rede[338], bem como a prevenção e combate à sua violação.

4.2.2.4 Resultados encontrados frente a disposição regulatória do Decreto nº 8.771/2016

Analisados pois os referidos artigos, é possível condensar os resultados alcançados da seguinte maneira: 1) o Decreto foi impreciso na distribuição das competências regulatórias, demandando esforço interpretativo e em conjunto com outros diplomas legais para a retirada de algum sentido da norma; 2) a Anatel não tem competência regulatória em matéria de dados pessoais no âmbito dos serviços que o monetizam, de forma central e abrangente (de modo a alcançar todo e

[336] "Apesar das intenções de vanguarda do referido decreto, a implementação destas medidas enseja um custo que nem sempre é considerado pelo legislador, bem como parece não se ter a completa noção dos custos com a fiscalização. Diante de uma realidade de recursos escassos, cabe ao poder público tomar uma decisão alocativa, de modo a priorizar os interesses sociais relevantes, estando dentre eles, a proteção da privacidade no meio digital." PASSOS, op. cit., p. 95

[337] "No mês de abril de 2017, foram registradas 258,8 mil reclamações na Agência Nacional de Telecomunicações (Anatel), queda de 19,9% na comparação com abril de 2016. Todos os principais serviços de telecomunicações apresentaram redução: a telefonia móvel, com 125,6 mil reclamações (-14,1%), a telefonia fixa, com 54,9 mil (-31,8%), a banda larga fixa, com 39,7 mil (-21,4%), e a TV por Assinatura, com 37,1 mil (-15,5%)." AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Reclamações registradas na Anatel caem 19,9% em abril.** Disponível em: <http://www.anatel.gov.br/institucional/noticias-destaque/1613-reclamacoes-registradas-na-anatel-caem-19-9-em-abril>. Acesso em: 12 jun. 2018.

[338] "a neutralidade da rede é um princípio de arquitetura de rede que endereça aos provedores de acesso o dever de tratar os pacotes de dados que trafegam em suas redes de forma isonômica, não os discriminando em razão de seu conteúdo ou origem". RAMOS, Pedro Henrique Soares. Neutralidade da rede e Marco Civil da Internet: um guia para interpretação. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014. pp. 165-187. p. 166

qualquer ente que monetize dados pessoais), restringindo-se, *in casu*, às hipóteses nas quais seus entes regulados utilizem os dados pessoais de seus usuários, bem como às que envolvam questões relativas à neutralidade da rede; 3) apesar de expressamente prevista no art. 18, a Senacon carece de meios eficazes para regulação em termos de dados pessoais, mormente por inexistir, dentre seus órgãos conformadores, ente centralizador que conjugue as funções próprias de agente regulatório e que possua considerável aporte técnico para tanto; 4) o CDC oferece certa guarida ao consumidor no que tange à proteção dos dados pessoais, principalmente em relação a informações claras sobre termos de uso e licenças (com destaque às cláusulas que impliquem em limitação de direito, como as que exploram a privacidade do usuário), ao livre acesso aos próprios dados e à possibilidade de correção dos mesmos (podendo, nestes termos, o usuário que se sinta violado em seus direitos acionar a justiça, buscar o Procon ou mesmo oferecer denúncia ao Ministério Público); 5) o SBDC não tem competência para regular em matéria de dados pessoais, limitando-se às hipóteses concernentes à neutralidade da rede (relacionadas, todavia, à violação da livre concorrência ou outra atribuição que lhe compita); 6) o CGI.br é órgão de caráter técnico-orientador, não possuindo as características conformadoras de um ente regulatório e é, portanto, incompetente para regular nesta matéria (apesar de influir e nortear, através de seu *know-how* (em tradução livre, "saber como", "conhecimento prático") técnico, os órgãos de fato competentes para tanto); e 7) inexiste órgão regulador específico que abranja a densa complexidade[339] do cenário de monetização de dados pessoais para efetivar a proteção destes dados e a garantia da privacidade no âmbito da internet, carência que poderia ter sido suprida com a sanção sem vetos da LGPD; 8) a criação da Autoridade Nacional de Proteção de Dados supriria essa defasagem e tornaria mais clara a distribuição de competências em matéria de monetização de dados pessoais, uma vez que tal Autoridade centralizaria, em sua maior parte, a competência para tanto.

4.2.3 Possibilidades de tutela da privacidade e de proteção dos dados pessoais diante do ferramental disponível

Como se pôde ver, o Brasil encontra-se ainda carente de ente regulador próprio em matéria de monetização de dados pessoais. Neste cenário, as alternativas restantes aos usuários de serviços *online* que sintam-se lesados em matéria de dados pessoais se restringem às já apontadas

[339] "A partir do comando do Marco Civil, que prestigia a competência do Comitê Gestor da Internet (CGI.br) ao propor diretrizes técnicas para o uso e desenvolvimento da Internet, o Decreto detalha o diálogo regulatório ampliado que deve existir para a melhor regulação e governança da rede no Brasil. Afirmando ainda as respectivas atribuições do Conselho Administrativo de Defesa Econômica (CADE), da Secretaria Nacional de Defesa do Consumidor (SENACON) e da Agência Nacional de Telecomunicações (ANATEL), o Decreto fortalece o entendimento de que as decisões que impactam a rede devem respeitar a diversidade que caracteriza a própria Internet." SOUZA; LEMOS, op. cit., p. 31

ferramentas oferecidas pelo Código de Defesa do Consumidor (acionando, por exemplo, o Procon ou exercendo, extrajudicialmente, as prerrogativas conferidas pelo art. 43 do CDC) e, no âmbito das empresas de telecomunicações, recorrer à Anatel para que esta tome as eventuais e necessárias medidas contra os entes por ela regulados.

Não obstante, há ainda a via do judiciário, que, inclusive, vem sendo utilizado no País tanto em casos particulares como em demandas de cunho coletivo. Atua, assim, de maneira subsidiária, sendo objeto projetor de sombra incluído forçadamente na equação em termos de luz e sombra.

A título exemplificativo, o processo de nº 1023161-81.2016.8.26.0577, que tramitou no Tribunal de Justiça de São Paulo e no qual a parte autora requereu a exclusão de seus dados pessoais de uma determinada aplicação da internet[340]; o processo nº 0218767-85.2009.8.19.0001 (número original), julgado no Superior Tribunal de Justiça e que tratou da exclusão de dados pessoais e do direito ao esquecimento[341]; e o processo nº 1015417-71.2017.8.26.0004, também tramitado no Tribunal de Justiça do Estado de São Paulo, no qual um motorista que tentou cadastrar-se em aplicativo de transporte não o conseguiu em razão de seus dados já terem sido previamente utilizados por terceiro[342].

De outra banda, o Ministério Público Federal já acionou a *Microsoft* e o *Google* em sede de Ações Civis Públicas, pleiteando a proteção dos dados pessoais dos usuários de maneira coletiva em razão de serviços oferecidos por estas companhias.

---

[340] BRASIL. Tribunal de Justiça do Estado de São Paulo. "Relação entre usuário e aplicação na internet - PAGSEGURO. Lei 12.965/14 – Marco Civil da Internet. Direito à exclusão dos dados pessoais mantidos pela aplicação da internet – art. 7º, X. Direito à privacidade. Dever de exclusão após o término da relação entre as partes. Sentença parcialmente mantida. Recurso Parcialmente Provido". **Nº 1023161-81.2016.8.26.0577**. Relator(a): Ana Paula Theodosio de Carvalho. Órgão Julgador: 2º Turma Cível, Foro Central Cível - 2ª VC F Reg Santo Amaro/SP. Data do Julgamento: 15/12/2017; Data de Registro: 15/12/2017. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=816005&cdForo=9012>. Acesso em: 13 jun. 2018.

[341] BRASIL. Superior Tribunal de Justiça. "Recurso especial. Direito civil. Ação de obrigação de fazer. 1. Omissão, contradição ou obscuridade. Ausência. 2. Julgamento extra petita. Não configurado. 3. Provedor de aplicação de pesquisa na internet. Proteção a dados pessoais. Possibilidade jurídica do pedido. Desvinculação entre nome e resultado de pesquisa. Peculiaridades fáticas. Conciliação entre o direito individual e o direito coletivo à informação. 4. Multa diária aplicada. Valor inicial exorbitante. Revisão excepcional. 5. Recurso Especial parcialmente provido". **RECURSO ESPECIAL Nº 1.660.168 – RJ**. Brasília. Data do julgamento: 05 de maio de 2018. Data da publicação: 05 de junho de 2018. Disponível em: <http://www.omci.org.br/m/jurisprudencias/arquivos/2018/stj_02187678520098190001_08052018.pdf>. Acesso em: 14 jun. 2018.

[342] BRASIL. Tribunal de Justiça do Estado de São Paulo. **Obrigação de Fazer - nº 1015417-71.2017.8.26.0004**. Requerente: P. H. B. S.. Requerida: UBER do Brasil Tecnologia Ltda. FORO REGIONAL XI – PINHEIROS, São Paulo/SP. Data do julgamento: 12 mar. 2018. Data da publicação: 15 mar. 2018. Disponível em: <http://www.omci.org.br/m/jurisprudencias/arquivos/2018/sp_10154177120178260004_12032018.pdf>. Acesso em: 14 jun. 2018.

No âmbito do feito de nº 5009507-78.2018.4.03.6100[343], o MPF combate a prática da Microsoft de coletar dados pessoais dos usuários do software "*Windows* 10" sem observância das determinações contidas no Marco Civil da Internet, requerendo que a demandada tome providências necessárias para adequar todas as licenças e/ou *softwares* do sistema operacional mencionado – sobretudo em relação ao consentimento claro e inequívoco, previsto no art. 7º, inciso VIII, do Marco Civil.

Já nos autos de nº 0025463-45.2016.4.01.4000, o MPF requer que o *Google* suspenda "a análise (escaneamento) do conteúdo dos e-mails dos usuários do *Gmail*, em todo o território nacional, enquanto não for colhido o consentimento prévio, expresso, e destacado do titular da conta de e-mail, inclusive para o envio de publicidade comportamental"[344], com base igualmente no art. 7º do Marco Civil da Internet.

Assim, na salvaguarda de seus direitos, aos usuários é permitida a busca pela solução de suas demandas no judiciário, sejam elas de maneira individual ou por meio de denúncias junto ao Ministério Público Federal, que poderá ingressar com ações de tutela coletiva de direitos.

Por tudo que já se expôs, a criação de uma lei geral de proteção de dados pessoais para o Brasil é de vital importância para suprir as lacunas previamente apontadas; é significativa, sobretudo e como previamente se pôde adiantar, porque o já aludido PLC 53/2018 prevê a criação da Autoridade Nacional de Proteção de Dados, que será formatada nos moldes da lei n 9.986/2000 e, portanto, contará com as competências, prerrogativas e poderes inerentes a uma agência reguladora e podendo, desta forma, fiscalizar a observância das normas protetoras dos dados pessoais, da privacidade[345] e aplicar sanções em caso de descumprimento das normativas atinentes à monetização de dados pessoais no Brasil.

---

[343] BRASIL. 9ª Vara Cível da Justiça Federal de São Paulo. **Ação Civil Pública – nº 5009507-78.2018.4.03.6100**. Requerente: Ministério Público Federal. Requerida: Microsoft Informática LTDA, União. Juíza Federal Cristiane Farias Rodrigues dos Santos. Data de julgamento: 27 abr. 2018. Data de publicação: 27 abr. 2018. Disponível em: <http://www.omci.org.br/m/jurisprudencias/arquivos/2018/jfsp_50095077820184036100_27042018.pdf>. Acesso em: 13 jun. 2018.

[344] BRASIL. 2ª Vara Federal de Teresina, Piauí. **Ação Civil Pública – 0025463-45.2016.4.01.4000.** Requerente: Ministério Público Federal. Requerida: Google Brasil Internet LTDA. Juiz Federal Márcio Braga Magalhães. Data de julgamento: 29 jan. 2018. Data de Publicação: 29 jan. 2018. Disponível em: <http://www.omci.org.br/jurisprudencia/189/escaneamento-de-emails-e-consentimento-previo/>. Acesso em: 13 jun. 2018.

[345] "A desestatização da economia, muitas vezes benéfica à coletividade e necessária à eficiência do Estado, não deve resultar na redução do âmbito de incidência dos direitos fundamentais, pois a história prova que o mercado não é suficiente para a proteção do mais fraco". SARMENTO, Daniel. **Direitos Fundamentais e Relações Privadas**. 2ª ed. Rio de Janeiro: Lumen Juris, 2010. p. 35

4.3 PERSPECTIVAS REGULATÓRIAS PARA A MONETIZAÇÃO DOS DADOS PESSOAIS NO BRASIL

Da análise até aqui empreendida, pôde-se aferir que, apesar da edição da LGPD regulamentando e garantindo a proteção dos dados pessoais no país, existe todo um arcabouço legal conferindo um mínimo de proteção aos titulares destes dados. O Código de Defesa do Consumidor foi pioneiro neste sentido, e o Marco Civil da Internet estabeleceu princípios e diretrizes que, minimamente, abalizam as atividades que utilizam os dados pessoais como insumos – tanto o é que, conforme se demonstrou, existem exemplos jurisprudenciais da tutela dos direitos inerentes aos dados pessoais, tanto individual como coletivamente.

Entretanto, e como se pôde observar, inexiste ente central fiscalizador ou regulatório destas atividades, estando os atores econômicos que dos dados se valem, atualmente, agindo com certa esfera de independência e autonomia: pelo que se expôs, as operadoras reguladas pela Anatel, por exemplo, devem obediência a esta entidade; mas os provedores de aplicações de internet, de outra banda, devem em tese obediência aos mandamentos do MCI e do CDC, sem haver, contudo, agente fiscalizador e de *enforcement* (fiscalização, execução, aplicação) destas normativas. O Brasil perdeu uma excelente oportunidade para suprir esta falta em razão do veto à criação da ANPD.

Neste cenário, o titular dos dados encontra-se por vezes em situações de extrema vulnerabilidade[346], notadamente pelo caráter altamente técnico dos processos que envolvem o tratamento dos dados pessoais. Deve contar, pois, com certa "boa vontade" dos serviços em adimplir, voluntariamente, com as determinações legais, sobretudo quando se considera o "postulado da vontade técnica"[347]: ante a capacidade técnica do que pode ser feito e as zonas cinzentas legais e normativas, não há dúvidas de que aquilo que a tecnologia permite será efetivamente posto em prática.

Ora, até mesmo o caminho que o mouse faz na tela do computador[348] de seus usuários é rastreado pelo Facebook – quão profunda não é a capacidade de análise das empresas monetizadoras de dados pessoais? O que será que efetivamente lhes escapa?

---

[346] "A necessidade da tutela jurídica e da intervenção do Estado para a proteção do consumidor reside no fato de que o mercado, ao invés de contribuir para a superação da vulnerabilidade do consumidor, na realidade, acaba por fazer o contrário: reforça a sua vulnerabilidade e o desequilíbrio em face dos fornecedores. O mercado propicia o acesso desigual à informação, que implica relações de poder no seu interior e que reflete, por conseqüência, as relações de poder na sociedade. Assim, ele deve ser visto não como um espaço naturalizado e neutro para escolhas voluntárias e livres, mas como uma ordem de poder e riqueza, moldada a partir dos mecanismos legais e regulatórios instituídos". MENDES, 2008, op. cit., p. 125

[347] DONEDA, 2006, op. cit., p. 17

[348] BEJERANO, Pablo G. **Facebook confirma que rastreia até os movimentos do seu mouse.** Disponível em: <https://brasil.elpais.com/brasil/2018/06/14/tecnologia/1528970968_169921.html>. Acesso em: 24 jul. 2018.

Ademais, além de ser obrigado a anuir com contratos de adesão sem qualquer oportunidade de negociação ou barganha acerca de seus termos, o usuário das aplicações *online* não têm a capacidade de fiscalizar o que os serviços fazem com seus dados, que fim dão a eles, se estão guardados satisfatoriamente, se os dados são comercializados com outras empresas, se são cedidos a entes governamentais, etc. Os termos e políticas de privacidade, não raro, são vagos nas suas disposições, sem destacar, como determinam o CDC e o Marco Civil, os trechos em que explicam quais dados serão coletados e para que fim servirão.

Ante isto, e considerando os resultados aferidos, é cada vez mais flagrante a necessidade de criação de ente central regulador, capaz de garantir a proteção dos dados pessoais e de conjugar o expertise técnico necessário às prerrogativas próprias de um agente regulatório: editando atos, fiscalizando sua aplicação e sancionando as possíveis violações, tudo em adequação e consonância às complexidades que a monetização de dados enseja e sem limitar as liberdades que a sociedade em rede proporciona. A perspectiva de criação da Autoridade Nacional de Proteção de Dados, ainda que tardia, neste desiderato, é esperança de otimismo para o cenário de monetização de dados pessoais, conferindo maior segurança jurídica aos modelos de negócio e imprimindo maior força à proteção dos direitos dos usuários de serviços na internet.

Em retrospecto: esboçamos a privacidade como direito fundamental, necessário de contextualização[349] para projetar conteúdo protetivo e baseado em uma qualidade perene, a liberdade, direito fundamental do qual deriva e também permeia; os dados pessoais, espalhados, coletados e utilizados no âmbito da sociedade em rede, ostentam a capacidade de conformar aspectos privados da vida de seus titulares, ensejando diversos riscos à privacidade e aos valores conexos destes.

Nesse cenário, a regulação é medida premente, que surge como um sopro de soberania e de retomada de poder decisório dos cidadãos ante a complexidade nesta conjuntura, nesta perspectiva intercruzada de interesses, vontades e forças – como o balançar da funda de Davi ante o Golias do ciberespaço; como a vingança do elo mais fraco dentre os nós que conformam as redes da Era da Informação.

A atuação do Estado ao estabelecer balizas, ainda que mínimas, ainda que parcamente eficazes, é legitimar o contrato social avençado pelas coletividades e que as lógicas da rede parecem subverter[350]. É salvaguardar o que Marcel Leonardi, Daniel Solove, Danilo Doneda e também, à sua

---

[349] "Não há, portanto, uma fórmula pronta capaz de determinar, prima facie, o peso que deve ser atribuído à privacidade. Em outras palavras, a privacidade não tem um valor uniforme em todos os contextos, sendo impossível escapar da necessidade da análise das circunstâncias do caso concreto […]". LEONARDI, op. cit., p. 113

[350] "Assim, o Estado-nação, com sua soberania e autoridade, é antagonizado pelos influxos dos diversos poderes que também são nós da rede, como acontece, por exemplo, quando informações sobre as atividades dos indivíduos nas suas vidas cotidianas circulam livremente entre as empresas que monetizam esses dados, sem a possibilidade de controle

maneira, Byung-Chul Han, chamaram de valor social da privacidade[351] – essa dimensão da liberdade de se desenvolver livremente, sem receios repressivos, de contestar, de ser diferente, de divergir[352], valor que é, inclusive, um dos fundamento da inovação em seu sentido mais amplo.

Neste azo é que se apontam duas posturas regulatórias pertinentes para o trabalho e adequadas ao panorama sob exame: são posturas que poderão atuar independentemente do modelo regulatório adotado (considerada, por óbvio, a presença do Estado em tal modelo) e que trazem em si características suficientemente genéricas e atemporais[353] para servirem à temática da regulação da monetização de dados pessoais – a chamada regulação do risco e o "*code is law*". Interpreta-se estes dois paradigmas como precisos porque abarcam proposituras intimamente relacionadas à proteção da privacidade nos termos sob os quais trabalhou-se até agora.

4.3.1 Os dados como o novo urânio, regulação do risco, "code is law" e outros apontamentos para uma regulação da monetização de dados pessoais observadora e protetora da privacidade e de seus valores conexos

Neste ponto, impende mencionar que os esforços anteriores na busca pela efetivação do direito à privacidade não devem ser desconsiderados ou postos de lado; pelo contrário, as proposições realizadas neste tópico visam a somar com as soluções já produzidas pelos estudiosos da temática e legisladores. Desta maneira, deve-se ter em mente que propostas como a anonimização de dados, a autodeterminação informativa, a necessidade de consentimento, entre outras, devem ser pensadas em conjunto quando teorizamos e propomos em matéria regulação. Não custa ressaltar a premissa metodológica do trabalho – a salvaguarda dos direitos fundamentais, mormente a privacidade. Neste intento, como várias vezes afirmado, todo meio é válido e toda solução é bem-vinda.

---

pelo direito estatal. Logo, no contexto da sociedade em rede, continua a ser necessária uma teoria do Estado, visto que as relações de poder, embora não confinadas exclusivamente à esfera estatal, permanecem sendo parte de toda atividade do Estado". MENEZES NETO, op. cit., p. 70

[351] "A privacidade, entretanto, tem valor social: ela molda as comunidades sociais e fornece a proteção necessária aos indivíduos contra diversos tipos de danos e intromissões, possibilitando que desenvolvam sua personalidade e devolvam à sociedade novas contribuições. Evidentemente, nem todas essas contribuições serão úteis; sem privacidade, porém, nenhuma poderá florescer". LEONARDI, op. cit., p. 121

[352] "A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento positivo, indutor da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Neste papel, a vemos como pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos". DONEDA, op. cit., p. 142

[353] "A maioria dos problemas trazidos pelas novas tecnologias exige a aplicação de princípios gerais em lugar de regras específicas". LEONARDI, op. cit., p. 40

Isto superado, tem-se que a regulação do risco, como a própria nomenclatura sugere, consiste basicamente na tomada de medidas que visam projetar salvaguardas ante possíveis e eventuais perigos oriundos de determinada atividade. Risco, nesta perspectiva, é a chance de um perigo vir a ocorrer[354]. Destarte, a regulação do risco seria uma ferramenta adequada para basear decisões a serem tomadas em face dos perigos em potencial.

É propositura que surge, inclusive, na esteira da preocupação com o meio ambiente e sua preservação[355]. Não é difícil imaginar o porquê, ainda mais quando já se vem fazendo analogias do uso dos dados pessoais com a indústria do petróleo e gás, extremamente nociva e degradante para com o ambiente que lhe circunda, e com a comparação com um material radioativo, que requer atenção e cuidados ainda mais intensos.

Assim é que associamos a analogia dos dados pessoais como o "novo urânio" à perspectiva da regulação do risco: considerando que o uso dos dados pessoais ostenta os já mencionados perigos à privacidade[356] dos seus titulares e dos valores a ela conexos – que vão desde a liberdade de pensamento, de crença, o livre desenvolvimento da personalidade, a liberdade política, a cidadania[357] e democracia[358], e até mesmo a liberdade de ser 'diferente' (de fugir da violência da transparência, de Byung-Chul Han) – tal qual um material radioativo, e sabendo[359] das possibilidades de tais riscos e perigos, o regulador pode precaver-se e estipular previsões, princípios, orientações e normativas adequados a lidar com as contingências surgidas destes riscos.

---

[354] "Put simply, risk is the chance (understood as a probabilistic notion) that a danger (i.e., an event with harmful consequences) will happen.". GELLERT, Raphaël. Understanding data protection as risk regulation. Journal of Internet Law, vol., 18, n. 11, May 2015. pp. 3-15. p. 8

[355] "This comparison with environmental law should come as no surprise as it has been the pioneering right dealing with the regulation of risks and harms to the environment and human health. It has therefore spawned many original procedures, mechanisms, and provisions that deal with scientific and technological risks". Ibidem, p. 12

[356] "Diante do alargamento conceitual da privacidade, verifica-se que o usuário, ao navegar pela Internet, enfrenta uma série de fatores de risco que vilipendiam esse direito fundamental, através de variados meios de intrusão informática". ALMEIDA, Marcos Paulo Dias de. **www.privacidade.com/direito_fundamental**: a necessária proteção da vida paralela da pessoa no ciberespaço. Monografia (Graduação em Direito). Natal: UFRN, 2015. 95f. p. 45

[357] "Isso significa que não se deve entender a tutela da privacidade como a proteção exclusiva de um indivíduo, mas sim como uma proteção necessária para a manutenção da estrutura social. A privacidade não é valiosa apenas para a vida privada de cada indivíduo, mas também para a vida pública e comunitária. Como destaca Gustavo Tepedino, o direito à privacidade consiste em tutela indispensável ao exercício da cidadania". LEONARDI, op. cit., p. 122

[358] "No século XXI, no entanto, os sentimentos já não são mais os melhores algoritmos no mundo. Estamos desenvolvendo algoritmos superiores que utilizam um poder computacional inédito e bases de dado gigantescas. Os algoritmos do Google e do Facebook sabem não apenas como você se sente, como sabem 1 milhão de outras coisas a seu respeito das quais você mal suspeita. Consequentemente, você deveria parar de ouvir seus sentimentos e começar a ouvir esses algoritmos externos. De que valem eleições democráticas quando os algoritmos sabem como cada um vai votar, assim como as razões pelas quais uma pessoa vota em um partido de esquerda enquanto outra vota em políticos de direita? O humanismo ordenava: 'Ouçam seus sentimentos!'; o dataísmo agora ordena: 'Ouçam os algoritmos! Eles sabem como você se sente'". HARARI, op. cit., não paginado.

[359] "the notion of risk is twofold. On the one hand, it is about knowing dangers, and on the other hand, it is about controlling the dangers on which one has collected information (and it is precisely because they are known that one can act upon them). Risk is therefore both about knowing dangers and –using the latter knowledge to- controlling them". GELLERT, op. cit., p. 8

Os riscos inerentes à monetização desta nova matéria-prima radioativa, a partir dos diferentes pontos de luz emanados dos interesses presentes na sociedade em rede, pode, como se demonstra, afetar a privacidade e seus valores conexos[360].

A possibilidade de manipulação[361] dos discursos, da narrativa política, das ideologias que serão ou não propagadas, de quanta publicidade se dará a determinado fato político – tudo isto, conforme se demonstrou, é factível e, portanto, um risco; um risco que tem o condão de afetar o próprio tecido dos fluxos democráticos[362].

Se, como quer Harari, somos todos pequenos "chips"[363], partes de um enorme processador de informações que é a humanidade, nossos dados pessoais são os bits que descortinam os nossos aspectos arcanos e que possibilitam certa margem de controle sobre nós mesmos[364]; há que se regular, portanto, quais informações circulam por esses "chips", quem as está promovendo e com qual intento, sob pena de pôr em xeque as liberdades[365] e a própria democracia.

Desta forma, para nós, a atuação do Estado, seja qual for o modelo regulatório a ser escolhido, tem de tomar uma postura do risco em relação à monetização de dados pessoais e, neste intento, deve possuir capacidade normatizante suficiente para fazer valer a proteção da privacidade potencialmente descortinada e eventualmente danosa – tal qual um material radioativo, o agente que

---

[360] "data protection outlines a complex bundle of interests worthy of protection. Data protection bases upon a multi-dimensional understanding of fundamental rights and requires entirely new descriptions of the protected interests: in place of legally protected goods conceived of in an individualistic way, it is about individual legal positions in sociality, or, in other words: the individual's social positions to be protected by fundamental rights. The bundle of protected interests and positions must still be worked out in greater detail and will also have to be dynamically adapted time and again to new dangers". ALBERS, op. cit., p. 229

[361] "Hoje as indústrias da informação estão todas incorporadas em nossa existência de uma maneira sem precedentes na história econômica, envolvendo todas as dimensões de nossa vida nacional e pessoal – econômica, sim, mas também expressiva, cultural, social e política. Elas não estão apenas integradas de forma efetiva em qualquer transação; também decidem quais entre nós seremos ouvidos ou vistos, e quando, seja ele um inventor inspirado, um artista ou um candidato". WU, 2012, op. cit., não paginado.

[362] "Entre os homens, a fala – no amplo sentido constitucional, que vai além da simples comunicação oral ou até verbal – tem efeitos e propósitos que transcendem a mera utilidade comercial. Sua oferta e seu consumo podem alcançar uma dimensão espiritual garantindo que uma televisão não é proveitosamente descrita como uma torradeira que não torra, mas que exibe sons e imagens. Quando pensamos numa música, num filme, num discurso político ou numa conversa particular, estamos considerando manifestações com o potencial de alterar sensibilidades, de mudar vidas. Todos nós lemos ou vimos algo que nos deixou uma impressão indelével, impossível de quantificar em relação aos custos de produção e distribuição. Foi por isso que Joseph Goebbels definiu o rádio como "a arma espiritual do Estado totalitário". Por esse mesmo motivo, nos anos 1940, o regime nazista desenvolveu novas formas de mídia com a mesma intensidade que novas armas de destruição. Atrás de cada tirania ou genocídio há uma parceria silenciosa com algum tipo de mídia de massa". Ibidem, não paginado.

[363] "Do ponto de vista dataísta, podemos interpretar toda a espécie humana como um sistema único de processamento de dados, no qual indivíduos humanos servem como *chips"*. HARARI, op. cit., não paginado.

[364] "Forthese reasons, Serge Gutwirth and Paul Hert have warned that if it is "possible to control and steer individuals without the need to identify them, the time has probably come to explore the possibility of a shift from personal data protection to data protection tout court." In other words, we can no longer turn to anonymity (or, more accurately, pseudonymity) to pull datasets outside the remit of privacy regulations and debate". BAROCAS; NISSENBAUM, op. cit., p. 54-55

[365] "The challenge for our generation is to reconcile these two forces. How do we protect liberty when the architectures of control are managed as much by the government as by the private sector? How do we assure privacy when the ether perpetually spies? How do we guarantee free thought when the push is to propertize every idea? How do we guarantee self-determination when the architectures of control are perpetually determined elsewhere?". LESSIG, op. cit., p. xv

desejar monetizar os dados pessoais deve ter ciência[366] de que aquela atividade ostenta deveres, responsabilidades e riscos – riscos estes que o agente deve assumir tanto para atuar na prevenção de sua ocorrência, como na reparação em razão de violação de direitos tutelados.

É uma regulação que deve ser, portanto, severa, visando salvaguardar os direitos dos titulares dos dados, e que se demonstra adequada, ainda, para abordar a situação da privacidade como valor social em uma perspectiva hiperdimensionada – não são os dados somente de um indivíduo que ostentam riscos, mas, também, os dados de grupos e coletividades.

Em um exercício de pensamento mais abstrato, pensar as ideias propostas por Lawrence Lessig é pensar uma matriz simplificada e capaz de interoperabilidade entre direito e tecnologia. É, ao mesmo tempo – e paradoxalmente – pensar distante das tecnicidades jurídicas e trazer para dentro delas a tecnologia. Aqui, com base na ideia de Lessig, o trabalho permite-se propôr ideias tão inusitadas quanto ousadas para o futuro da regulação da monetização de dados pessoais.

Para Lessig, "*code is law*": é dizer, o código é lei. Em síntese, Lessig constrói uma concepção de que o código, por ser, em última instância, a representação da escolha de uma pessoa (ou pessoas), refletem valores[367], instâncias de poder[368] – é uma decisão política. Desta maneira, estando o código informático conformando estruturas e arquiteturas[369] que limitam as liberdades, acessos, comunicações, comportamentos, etc, estaria agindo tal qual o Direito em seu objetivo de regular a sociedade[370] (como, por exemplo, o Direito Penal regula o comportamento dos cidadãos para evitar delitos).

Portanto, se o código é lei, por quê não levar esta proposição além? Se o código é a representação de uma vontade, a representação de interesses, a representação de poderes; e se esses códigos, em uma perspectiva de regulação, devem obediência tanto quanto aos demais códigos, por

---

[366] "The architecture should also be premised on the notion that the collection and use of personal information is an activity that carries duties and responsibilities. The law should establish specific measures of control over entities maintaining systems of personal data. For example, if a company is providing background check information about a person, it should be held responsible for any inaccuracies or deficiencies in the information". SOLOVE, 2004, p. 121

[367] "Choices among values, choices about regulation, about control, choices about the definition of spaces of freedom—all this is the stuff of politics. Code codifies values, and yet, oddly, most people speak as if code were just a question of engineering. Or as if code is best left to the market. Or best left unaddressed by government". LESSIG, op. cit., p. 78

[368] "But the architecture of cyberspace is power in this sense; how it is could be different. Politics is about how we decide, how that power is exercised, and by whom". Ibidem, p. 78

[369] "Architecture is a kind of law: It determines what people can and cannot do. When commercial interests determine the architecture, they create a kind of privatized law. I am not against private enterprise; my strong presumption in most cases is to let the market produce. But isn't it absolutely clear that there must be limits to this presumption? That public values are not exhausted by the sum of what IBM might desire? That what is good for America Online is not necessarily good for America?". LESSIG, op. cit., p. 77-78

[370] "The code or software or architecture or protocols set these features, which are selected by code writers. They constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. In this sense, it too is regulation, just as the architectures of real-space codes are regulations". Ibidem, p. 124-125

exemplo, à Constituição, por quê não considerar as linhas de códigos linhas legais em seu sentido lato?

Seria possível, por exemplo, pensar na criação e exigência, por parte da autoridade reguladora competente, de uma espécie de estatuto eletrônico – um "E-statuto" – instrumento legal que serviria de intermediário entre as normas informadoras da regulação, tais quais as já trabalhadas e previstas na Constituição, no Marco Civil da Internet, no Decreto nº 8.771/2016, no Código de Defesa do Consumidor e na Lei Geral de Proteção de Dados Pessoais, e entre as linhas de código informático propriamente ditas criadas e geridas pelas companhias que monetizam dados pessoais; seria levar o "*privacy by design*", a prática de incutir proteções à privacidade nos procedimentos das instituições, ao extremo.

Desta maneira, haveria uma conexão direta entre lei e código, de forma que seria possível, até mesmo, suscitar a inconstitucionalidade de linhas de código informático que não se adequassem às previsões constitucionais (tais quais, por exemplo, as do art. 5º, X, XI e XII). Para usar de mais uma analogia, tal "estatuto eletrônico" atuaria como a máquina que conectava os humanos "reais" ao mundo fantasioso da Matrix[371]; seria o liame entre o legal e o tecnológico, entre o físico e o digital, entre o ser e o dever-ser – entre a legitimação do poder político que emana do povo e a arquitetura de poder do código informático.

Continuando nesta lógica, é possível pensar, ainda, na existência de códigos, programas e algoritmos criados pelo Estado para atuar na promoção, defesa e fiscalização dos direitos dos titulares dos dados pessoais. Imagine-se, ainda na lúdica do filme Matrix, uma espécie de "Agente Smith[372]": é possível imaginar a atuação de algoritmos capazes de verificar possíveis violações de direitos, aferir vazamentos de dados, de fiscalizar o *compliance* das empresas, de conferir se as perspectivas de anonimização, por exemplo, estão sendo realizadas (e se com a efetividade necessária para minimizar os riscos); programas capazes de verificar a *accountability*, aferindo se, por exemplo, relatórios e balanços fornecidos pelos entes regulados dizem a verdade, se estão se adequando aos princípios como o da finalidade, adequação ou necessidade[373], etc.

Quanto às possíveis críticas, nos atemos a rebater de antemão apenas aquela que é a mais frequente e, portanto, passível de se prever: a dos custos.

---

[371] THE MATRIX (Matrix), Direção e roteiro: Andy Wachowski e Larry Wachowski, Produção Joel Silver. Distribuição: Warner Bros. EUA, 1999.

[372] Personagem que representava o software "mantenedor da ordem" dentro da "Matrix", e que caçava aqueles que infrigiam a ordem imposta.

[373] Art. 6º da LGPD: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados".

Por este lado, parte-se da premissa de que é preciso uma Autoridade Nacional de Proteção de Dados, com poderes e capacidades técnicas suficientes para produzir estas ousadas sugestões; neste horizonte, sendo autarquia especial integrante da administração pública federal indireta, contaria como receita com as dotações consignadas no orçamento geral da União, além de outras fontes de renda típicas de uma agência reguladora.

Este orçamento, aliado a um *know-how* altamente especializado – e que contará, ainda, com o apoio do CGI.br – será capaz de produzir modelos padrões de "E-statutos", a serem oferecidos gratuitamente para quem as quisesse. Assim, tanto grandes companhias como pequenas *startups* teriam as mesmas possibilidades de adequarem-se aos parâmetros instituídos pela futura ANPD. Igualmente democrática seria a atuação dos algoritmos públicos, podendo ser inclusive disponibilizadas linhas-códigos padrões para facilitar o *compliance* e a interoperabilidade entre regulador e regulados. Isso, inclusive, rebateria as críticas de mitigação da inovação, uma vez que os meios e ferramentais normatizadores estariam disponíveis a qualquer um que desejasse.

Por quê decretar a falência do Estado ante esta conjuntura? Por quê não pensar em levar o Estado para dentro da tecnologia, buscando proteger os direitos fundamentais no âmbito da sociedade em rede? Já há quem fale, inclusive, sobre a necessidade de novos profissionais nesta área[374], capazes de atuar sob essa perspectiva multidisciplinar. Juristas que consigam unir Códigos e código; que programem o Direito; que legalizem os códigos.

O próprio Lessig já dizia que alcançar o *mix* adequado entre lei e tecnologia era a medida de se lograr níveis eficientes de "regulabilidade" (entendida como a capacidade ótima de se regular). Pensar da forma como sugerimos, então, seria levar à literalidade – e além – a propositura do jurista norte-americano. Afinal, diante da "vontade da técnica", pouco há o que fazer senão adaptar-se; se permite, então, imaginar até mesmo uma nova categoria de atos administrativos, levando o Estado, e os direitos, deveres, prerrogativas e garantias nele subentendidas para o ciberespaço.

Na perspectiva deste trabalho, esta ousada propositura seria elevar os níveis de eficiência da regulação, posto que levaria a fiscalização, por exemplo, ao preciso lugar onde esta deveria ocorrer. Correições, auditorias e outros procedimentos fiscalizatórios ocorreriam nas linhas de códigos, nos *bytes*, nos algoritmos e programas, e não mais diante de uma sala de reunião, repleta de folhas de papel e de pessoas com um intento nem sempre autêntico.

Desde que asseguradas as capacidades técnicas e a eficiência destes algoritmos públicos, estariam alijadas (ou, no mínimo, reduzidas) do processo regulatório as possibilidades de erro humano e de interferências humanas ilegítimas na atuação da autoridade regulatória, por exemplo.

---

[374] PÁDUA, Luciano. **'Precisamos de uma geração de engenheiros legais', diz Richard Susskind**. Disponível em: <https://www.jota.info/carreira/susskind-futuro-direito-05062018>. Acesso em 25 jun. 2018.

Os pontos de luz, potenciais violadores da privacidade e de seus valores conexos, surgidos da “vontade da técnica” e todas as possibilidades que esta enseja, estariam à mercê igualmente da própria vontade da técnica. Descortina-se, nesta verdadeira tentativa de equiparação de poderes, mais uma dimensão paradoxal desta propositura, na medida em que se retira deste processo o elemento humano precisamente para se garantir direitos humanos e prerrogativas fundamentais dos titulares de direito.

5 CONCLUSÕES

A tarefa a que se dedicou o presente trabalho mostrou-se, desde as primeiras linhas, um desafio árduo e complexo. Tratou de temas tão aparentemente distintos quanto repletos de nuances, críticas e problemáticas próprias. Todavia, acredita-se que logrou alcançar, minimamente, aos objetivos inicialmente propostos.

Assim é que, no capítulo de número dois, o trabalho tratou do direito à privacidade e suas inúmeras complexidades. Viu-se como este direito surgiu no âmbito da revolução burguesa e das demandas surgidas com esta nova classe social dominante, desenvolvendo-se à medida em que igualmente desenvolviam-se os aparatos e soluções tecnológicas da sociedade.

Pôde-se demonstrar como este direito foi informado por doutrina e jurisprudência em tentativas de conformação do seu conteúdo para abordar as diferentes problemáticas, dando gênese, primeiramente, aos conceitos monistas de direito à privacidade – o direito a estar só, o direito de proteção contra intrusão de terceiros, a dicotomia público x privado, a proteção do sigilo de informações e a autodeterminação informativa – e teorias de proteção e tutela, como a teoria das esferas.

Adiante, argumentou-se como o paradigma da sociedade informacional, pautada cada vez mais no protagonismo dos dados e das informações, lançou luz para a necessidade de proteção dos dados pessoais como elemento corolário do direito à privacidade, em razão da capacidade que o tratamento destes tem para descortinar aspectos íntimos e privados dos titulares, pondo em risco, igualmente, valores inerentes à privacidade – notadamente a liberdade e as prerrogativas que esta encerra.

Defendeu, ante esta complexidade de se conceituar a privacidade, uma acepção abstrata e baseada em uma qualidade perene mínima para sua conformação e que abarcasse as distintas acepções deste direito: a liberdade. Esboçou-se a metáfora em termos de luz e sombra para explicitar como o conteúdo protetivo da privacidade, a sombra, projetada pelos diplomas e institutos legais que a tutelam, possui a liberdade de amoldar-se de acordo com as situações específicas, apontando, destarte, a necessidade de contextualização para preenchimento do conteúdo protetivo deste direito; os pontos de luz, que nesta metáfora representam os riscos de violação da privacidade, são os elementos faltantes nesta contextualização.

Ponderou-se que esta concepção de privacidade seria adequada para atender às situações advindas da monetização de dados pessoais precisamente por pautar-se na liberdade inerente à sombra, capaz de modelar-se de acordo com a luz, de forma que este constructo alcança, ante a

argumentação construída, a capacidade protetiva necessária frente a complexidade do cenário estudado.

No capítulo de número três, procurou-se delinear o cenário no qual encontra-se inserta a atividade de monetização dos dados pessoais; de um lado, demonstrando a complexidade das relações que ostenta, e, de outro, buscando expôr em termos mais práticos como seriam os pontos de luz, os potenciais violadores da privacidade e de seus valores conexos.

Explicitou como diferentes autores debruçaram-se e criaram nomenclaturas para o cenário de protagonismo dos dados e da informação. Explicou o que se entende por sociedade da informação e sociedade em rede, delineando o papel central que a informação toma neste paradigma, permeando, influenciando e nutrindo um sistema cada vez mais interconectado e global de fluxos, interesses e vontades; como ensinou Manuel Castells, as indústrias agora passam a encontrar valor na informação, e esta permeia os inúmeros outros setores da sociedade, como a economia, a política, a sociologia, a cultura, os relacionamentos e comportamentos humanos.

A este fenômeno, como relatado, Andrew Murray chamou de convergência digital, explicitando a mudança do valor dos átomos para os *bytes.* Demonstrou-se, igualmente, o que se entende por ciberespaço, como trabalharam John Perry Barlow, Lawrence Lessig, Pierre Lévy e Daniel Solove, e em como neste ambiente digital, formado por instrumentos computacionais interligados por uma rede de alcance mundial, se pautam as diversas relações – sejam elas sociais, econômicas e até mesmo políticas.

Explicou-se que, para o intento inicial do trabalho, tais definições serviriam apenas de base para explanar o paradigma no qual encontra-se inserida a monetização de dados pessoais, de forma que ficassem explícitas algumas características básicas, como o protagonismo das Tecnologias da Informação e da Comunicação, da internet, dos dados e das informações e do valor que ostentam estes dados e informações, a intensa e profusa interconectividade, a dinâmica de fluxo das redes, o caráter supranacional das redes e as dificuldades que tal situação traz.

Colocadas tais características, passou-se a elaborar alguns exemplos práticos de como se dá a monetização de dados pessoais, de forma a situar pragmaticamente o trabalho e a representar os pontos de luz da metáfora proposta, elaborando sobre seus riscos e perigos.

Defendeu-se, a partir da constatação do valor atribuído aos dados pessoais e dos perigos que esta atividade ostenta, que os dados não são o novo petróleo mas, sim, o novo urânio, em razão dos perigos potenciais à privacidade e a seus valores conexos, como o livre desenvolvimento da personalidade, a liberdade de pensamento, liberdade de crença, liberdade sexual, liberdade política, entre outros. Partindo igualmente desta constatação é que se argumentou pela necessidade de

regulação das atividades monetizadoras de dados pessoais, com a finalidade de proteger a privacidade e seus valores conexos.

No capítulo de número quatro, estudou-se as possibilidades e perspectivas regulatórias diante deste cenário. Inicialmente, ressaltou-se as dificuldades e desafios que se dispõem ante esta tarefa, explicitando a posição de debilidade do Estado no âmbito das redes e a vulnerabilidade em que se encontra o titular dos dados pessoais nesse cenário – de forte influência de grandes companhias, que veem nesses dados a sua fonte de riqueza.

Defendemos, ante isto, a necessidade de presença e de retomada de força do Estado na sociedade em rede, com intuito de fazer valer os direitos dos titulares dos dados pessoais, pugnando por uma regulação estatal ativa e poderosa.

Arrazoou-se que o vigor da imposição normativa emanada pela regulação estatal deve ser extremamente intenso, sobretudo ante aos interesses concorrentes no contexto da monetização de dados pessoais e pela necessidade de proteção do direito fundamental à privacidade. Neste panorama, a regulação do risco, atribuindo a característica de metal radioativo ao uso dos dados pessoais, nos surgiu como ferramenta que traduz uma força mínima para o cenário: de um lado, pois revitaliza a capacidade normativa e sancionatória do Estado nacional, que padece de força ante a globalização e seus fluxos supranacionais e, de outro, porque impõe aos interessados em manusear os dados pessoais medidas apriorísticas de regulação severas, intensas, construindo instrumentos sancionatórios e responsabilizadores igualmente severos.

Verificou-se que, apesar da edição de lei específica de proteção de dados pessoais, a LGPD, capaz de normatizar a monetização destes dados, restou vetada e ausente a Autoridade Nacional de Proteção de Dados, órgão com caráter de agência reguladora única e centralizadora, capaz de atuar unicamente neste tema. Em razão disto, perscrutou-se os diplomas legais existentes na busca por uma competência regulatória mínima, capaz de fazer valer as prerrogativas e direitos dos titulares dos dados pessoais. Demonstrou-se que existe uma proteção fragmentada e setorizada, dividida entre entes como Anatel, Senacon e Judiciário, fato que, por si só, fragiliza a proteção dos dados pessoais e da privacidade.

Após a análise supramencionada, colheu-se e expôs-se alguns resultados – não somente em matéria regulatória, mas também de possibilidades de tutela da privacidade diante do ferramental disponível. Foi sugerido, como dito anteriormente, a atuação comedida da Senacon e da Anatel, assim como do Ministério Público Federal, em demandas coletivas; e do próprio indivíduo, em demandas particulares no Judiciário. Viu-se, todavia, que estas soluções não alcançam todas as situações advindas da complexidade da sociedade em rede e seus desafios (como os *cookies* e a transferência de dados entre empresas), motivo pelo qual o trabalho pugna pela criação da

Autoridade Nacional de Proteção de Dados para atuar, normatizar e regular, eficientemente, a monetização de dados pessoais no Brasil.

Por fim, buscando construir postulados genéricos, abstratos e principiológicos, capazes de alcançar a complexidade do tema e possuir uma atemporalidade que conferiria maior utilidade ao trabalho, foram propostas algumas ideias – até mesmo um pouco ousadas – para a regulação desta atividade.

Partindo da premissa de que os dados são o novo urânio e considerando os riscos que, portanto, ostentam para os direitos fundamentais dos titulares dos dados, baseando-se também na regulação do risco e na ideia de que "*code is law*", o trabalho sugere um protagonismo diferente do Estado neste cenário: em vez de decretar sua falência e debilidade, sugerimos que o Estado aborde a questão do risco com a maior efetividade possível, fazendo valer a soberania da sociedade e dos titulares dos dados nos intensos e complexos fluxos da rede.

Sugeriu, também, que o Estado adentre o âmbito da tecnologia, que reinvente-se, que se adéque aos postulados da técnica para efetivar os direitos que almeja proteger. Se "o código é lei", a lei também poderia ser código, conjecturando institutos que façam a conexão entre os códigos informáticos e a lei – de forma que, por exemplo, uma linha de código de um software ou algoritmo deva obediência aos ditames constitucionais, sendo possível inclusive a declaração de sua inconstitucionalidade, caso não sejam compatíveis; sugeriu a criação de documentos chamados "E-statutos", imaginando um documento capaz de conectar o ciberespaço e seus procedimentos à lei e seus ditames. Imaginou-se igualmente a utilização de algoritmos públicos – produzidos pelo Estado – para substituir certas atividades da regulação tradicional, de forma que, v. g., a própria técnica seja utilizada para fiscalizar a técnica.

Acredita-se, assim, que o trabalho logrou alcançar os objetivos dispostos inicialmente: foi possível elencar as leis e normativas atinentes que abordam a monetização de dados pessoais no Brasil, apontando os entes e institutos regulatórios disponíveis, e sendo possível sugerir, nos termos propostos – gerais e abstratos – perspectivas para a regulação da monetização de dados pessoais no Brasil com vistas à proteção do direito fundamental à privacidade.

Pôde-se analisar, brevemente, a evolução do direito fundamental à privacidade até a proteção dos dados pessoais, mencionando, ainda, a existência dos valores conexos e que necessitam de proteção; foi possível abordar o panorama da monetização de dados, explicando o paradigma que lhe rege, esboçando exemplos de como esta atividade se dá na prática e como surge a preocupação com o direito fundamental à privacidade; o trabalho foi capaz de pincelar o cenário regulatório desta temática no Brasil, extraindo do corpo legal disponível capacidades regulatórias objetivando não apenas a proteção da privacidade, mas também de seus valores conexos; assim

como, igualmente, propôs e sugeriu apontamentos legais genéricos, axiológicos e atemporais capazes de lidar com relativa adequação com a complexidade do tema.

Como subproduto da pesquisa, foi possível aferir a existência de correntes doutrinárias distintas no estudo da proteção de dados pessoais e da privacidade. De um lado, estão aqueles que, assim como o presente trabalho, consideram a proteção dos dados pessoais como elemento corolário do direito fundamental à privacidade, tendo relação de subsunção entre si; de outro, estão aqueles autores que acreditam ser a proteção dos dados pessoais matéria muito mais ampla, que demanda debate próprio e apartado da privacidade, havendo ainda quem considere ser sua proteção uma nova espécie de direito fundamental.

Assim, acredita-se ter contribuído, ainda que timidamente, para a construção de um saber teórico apto a auxiliar no debate sobre a regulação da monetização de dados pessoais no Brasil. Teve-se plena ciência das complexidades inerentes ao tema, das dificuldades que ele apresenta e de que, invariavelmente, deixamos de apreciar uma ou outra posição teórica. Todavia, tem-se a convicção de que o esforço empreendido atendeu ao pressuposto crítico adotado, visando, em última análise, a proteção do direito à privacidade e dos seus valores conexos, sem ter tido, contudo, a intenção de esgotar esta vasta e instigante temática.

REFERÊNCIAS

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resolução nº 632, de 7 de março de 2014**. Aprova o Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações – RGC. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/2014/750-resolucao-632>. Acesso em: 30 out. 2017.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Reclamações registradas na Anatel caem 19,9% em abril**. Disponível em: <http://www.anatel.gov.br/institucional/noticias-destaque/1613-reclamacoes-registradas-na-anatel-caem-19-9-em-abril>. Acesso em: 12 jun. 2018.

ALBERS, Marion. **Realizing the Complexity of Data Protection**. In: GUTWIRTH, Serge, et al (eds.). **Reloading Data Protection**: Multidisciplinary Insights and Contemporary Challenges. Dordrecht (Holanda): Springer, 2014.

ALMEIDA, Marcos Paulo Dias de. **www.privacidade.com/direito_fundamental**: a necessária proteção da vida paralela da pessoa no ciberespaço. Monografia (Graduação em Direito). Natal: UFRN, 2015. 95f.

ALVES, Fabrício Germano. **Análise da possibilidade de regulação da publicidade comportamental (behavioral advertising) pelo microssistema consumerista**. Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo. Brasília, v. 2, n. 1, p. 208-223, Jan/Jun. 2016.

ARAGÃO, Alexandre Santos de. **Agências Reguladoras e a evolução do Direito Administrativo Econômico**. 3ª ed. Rio de Janeiro: Forense, 2013.

ARTIGO 19. **Proteção de dados pessoais no Brasil**: Análise dos projetos de lei em tramitação no Congresso Nacional. Coord.: Laura Tresca. São Paulo: Artigo 19, 2016. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>. Acesso em: 08 jul. 2018.

BAPTISTA, Patrícia; KELLER, Clara Iglesias. Por que, quando e como regular as novas

tecnologias? Os desafios trazidos pelas inovações disruptivas. **RDA – Revista de Direito Administrativo**, Rio de Janeiro, v. 273, p. 123-163, set./dez. 2016.

BARBOSA, Alexandre (Coord.). **Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro**: TIC governo eletrônico 2017. São Paulo: Comitê Gestor da Internet no Brasil, 2018. Disponível em: <http://www.cgi.br/media/docs/publicacoes/2/TIC_eGOV_2017_livro_eletronico.pdf>. Acesso em 10 jul. 2018.

BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run around Anonymity and Consent. In: LANE, Julia, et al. **Privacy, Big Data, and the Public Good**: Frameworks for Engagement. New York: Cambridge University, 2014. cap. 2, pp. 44-75.

BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Trad. Carlos Alberto Medeiros. Zahar: Rio de Janeiro, 2014.

BBC. **Edward Snowden: Leaks that exposed US spy programme**. Disponível em: <http://www.bbc.com/news/world-us-canada-23123964>. Acesso em: 14 set. 2017.

BEJERANO, Pablo G. **Facebook confirma que rastreia até os movimentos do seu mouse.** Disponível em: <https://brasil.elpais.com/brasil/2018/06/14/tecnologia/1528970968_169921.html>. Acesso em: 24 jul. 2018.

BENNETT, Madeline. **How data analytics can revolutionise healthcare**. Disponível em: <https://www.telegraph.co.uk/business/open-economy/how-data-analytics-can-revolutionise-healthcare/>. Acesso em 13 jul. 2018.

BIEGEL, Stuart. **Beyond our control?** Confronting the limits of our legal system in the age of cyberspace. Cambridge: MIT, 2001.

BIONI, Bruno Ricardo. Ecologia: uma narrativa inteligente para a proteção de dados pessoais nas cidades inteligentes. In: BARBOSA, Alexandre (Coord.). **Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro**: TIC governo eletrônico 2017. São Paulo: Comitê Gestor da Internet no Brasil, 2018. Disponível em:

<http://www.cgi.br/media/docs/publicacoes/2/TIC_eGOV_2017_livro_eletronico.pdf>. Acesso em 10 jul. 2018.

BOBBIO, Norberto. **A era dos direitos**. Trad. Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 2004.

BONNINGTON, Christina. .**This Is The Creepiest Facebook-Friend Suggestion Story Yet.** Disponível em: <https://www.refinery29.com/2016/08/121691/facebook-friend-suggestion-psychiatrists-office>. Acesso em: 01 jul. 2018.

BRASIL. 2ª Vara Federal de Teresina, Piauí. **Ação Civil Pública – 0025463-45.2016.4.01.4000**. Requerente: Ministério Público Federal. Requerida: Google Brasil Internet LTDA. Juiz Federal Márcio Braga Magalhães. Data de julgamento: 29 jan. 2018. Data de Publicação: 29 jan. 2018. Disponível em: <http://www.omci.org.br/jurisprudencia/189/escaneamento-de-emails-e-consentimento-previo/>. Acesso em: 13 jun. 2018.

_____. 9ª Vara Cível da Justiça Federal de São Paulo. **Ação Civil Pública – nº 5009507-78.2018.4.03.6100**. Requerente: Ministério Público Federal. Requerida: Microsoft Informática LTDA, União. Juíza Federal Cristiane Farias Rodrigues dos Santos. Data de julgamento: 27 abr. 2018. Data de publicação: 27 abr. 2018. Disponível em: <http://www.omci.org.br/m/jurisprudencias/arquivos/2018/jfsp_50095077820184036100_27042018.pdf>. Acesso em: 13 jun. 2018.

_____. Ministério do Planejamento, Desenvolvimento e Gestão. **CGI.br**. Disponível em: <https://www.governodigital.gov.br/transformacao/cgi-br>. Acesso em: 10 out. 2017.BRASIL. **Projeto de Lei da Câmara nº 53/2018**. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7738646&ts=1529700780674&disposition=inline&ts=1529700780674>. Acesso em: 24 jun. 2018.

_____. **Constituição (1988)**. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 29 out. 2017.

_____. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei no 12.965, de 23 de abril de

2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm>. Acesso em 20 out. 2017.

_____. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/l8078.htm>. Acesso em 20 out. 2017.

_____. **Lei nº 9.472, de 16 de julho de 1997**. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9472.htm>. Acesso em 21 out. 2017.

_____. **Lei nº 12.965, de 23 de abril de 2014.** Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 19 out. 2017.

_____. Presidência da República. Secretaria de Comunicação Social. **Pesquisa brasileira de mídia 2015**: hábitos de consumo de mídia pela população brasileira. Brasília: Secom, 2014.

_____. Ministério da Ciência, Tecnologia Inovações e Comunicações; Ministério do Planejamento, Desenvolvimento e Gestão; Banco Nacional do Desenvolvimento. **Relatório do plano de ação – capítulo regulatório:** Produto 8. Brasília, 2017.

_____. Superior Tribunal de Justiça. “Recurso especial. Direito civil. Ação de obrigação de fazer. 1. Omissão, contradição ou obscuridade. Ausência. 2. Julgamento extra petita. Não configurado. 3. Provedor de aplicação de pesquisa na internet. Proteção a dados pessoais. Possibilidade jurídica do pedido. Desvinculação entre nome e resultado de pesquisa. Peculiaridades fáticas. Conciliação entre o direito individual e o direito coletivo à informação. 4. Multa diária aplicada. Valor inicial exorbitante. Revisão excepcional. 5. Recurso Especial parcialmente provido”. **RECURSO**

ESPECIAL Nº 1.660.168 – RJ. Brasília. Data do julgamento: 05 de maio de 2018. Data da publicação: 05 de junho de 2018. Disponível em: <http://www.omci.org.br/m/jurisprudencias/arquivos/2018/stj_02187678520098190001_08052018.pdf>. Acesso em: 14 jun. 2018.

_____. Tribunal de Justiça do Estado de São Paulo. "Relação entre usuário e aplicação na internet - PAGSEGURO. Lei 12.965/14 – Marco Civil da Internet. Direito à exclusão dos dados pessoais mantidos pela aplicação da internet – art. 7º, X. Direito à privacidade. Dever de exclusão após o término da relação entre as partes. Sentença parcialmente mantida. Recurso Parcialmente Provido". **Nº 1023161-81.2016.8.26.0577**. Relator(a): Ana Paula Theodosio de Carvalho. Órgão Julgador: 2º Turma Cível, Foro Central Cível - 2ª VC F Reg Santo Amaro/SP. Data do Julgamento: 15/12/2017; Data de Registro: 15/12/2017. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=816005&cdForo=9012>. Acesso em: 13 jun. 2018.

_____. Tribunal de Justiça do Estado de São Paulo. **Obrigação de Fazer - nº 1015417-71.2017.8.26.0004**. Requerente: P. H. B. S.. Requerida: UBER do Brasil Tecnologia Ltda. FORO REGIONAL XI – PINHEIROS, São Paulo/SP. Data do julgamento: 12 mar. 2018. Data da publicação: 15 mar. 2018. Disponível em: <http://www.omci.org.br/m/jurisprudencias/arquivos/2018/sp_10154177120178260004_12032018.pdf>. Acesso em: 14 jun. 2018.

BUTIN, Denis; CHICOTE, Marcos; LE MÉTAYER, Daniel. **Strong Accountability**: Beyond Vague Promises. In: GUTWIRTH, Serge, et al (eds.). **Reloading Data Protection**: Multidisciplinary Insights and Contemporary Challenges. Dordrecht (Holanda): Springer, 2014. pp. 3-20.ll

CARVALHO FILHO, José dos Santos. Agências reguladoras e poder normativo. **Revista Eletrônica de Direito Administrativo Econômico**, Salvador, Instituto Brasileiro de Direito Público, nº 9, fev./mar./abr., 2007. Disponível em: <http://www.direitodoestado.com.br/redae.asp>. Acesso em: 15 de maio de 2017.

CASTELLS, Manuel. **A sociedade em rede**. Vol. 1. 8ª ed. Trad.: Roneide Venancio Majer. São Paulo: Paz e Terra, 2005.

CHERRY, Denny. **Fundamentos da privacidade digital**. Rio de Janeiro: Elsevier, 2015.

CRUZ, Everton Lima da; CARVALHO, V. M. B. Recursos hídricos na indústria do petróleo e gás: a produção e o descarte de água em plataformas. In: XAVIER, et. al (org.). **Proteção do meio ambiente na indústria do petróleo e gás natural**. Natal: EDUFRN, 2016.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. **Direito e Internet III**: Marco Civil da Internet. São Paulo: Quartier Latin, 2015.

DIAS, P. Y. Regulação da internet como administração da privacidade. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 9, n. 1, p. 167-182, maio de 2017.

DIMOULIS, Dimitri. MARTINS, Leonardo. **Teoria Geral dos Direitos Fundamentais**. 5ª ed. São Paulo: Atlas, 2014.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Rev. Espaço Jurídico,** Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

_____. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

_____; MENDES, Laura Schertel. Data protection in Brazil: New Developments and Current Challenges. In: GUTWIRTH, Serge, et al (eds.). **Reloading Data Protection**: Multidisciplinary Insights and Contemporary Challenges. Dordrecht (Holanda): Springer, 2014. p. 3-20.

DOSTOIÉVSKI, Fiódor. **Recordações da Casa dos Mortos**. Trad.: Nicolau S. Peticov. São Paulo: Nova Alexandria, 2005. Não paginado (epub).

DOWARD, Jamie; GIBBS, Alice. **Did Cambridge Analytica influence the Brexit vote and the US election?** Disponível em: <https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump>. Acesso em: 09 abr. 2018.

FARIA, José Eduardo. **Sociologia jurídica**: direito e conjuntura. 2. ed. São Paulo: Saraiva, 2010.

FREDRIKSSON, Torbjörn. Esforços necessários para transformar o comércio eletrônico em um

motor do desenvolvimento. In: BARBOSA, Alexandre (Coord.). **Pesquisa sobre o uso das tecnologias de informação e comunicação nas empresas brasileiras**: TIC empresas 2017. São Paulo: Comitê Gestor da Internet no Brasil, 2018. Disponível em: <http://www.cgi.br/media/docs/publicacoes/2/TIC_Empresas_2017_livro_eletronico.pdf>. Acesso em 10 jul. 2018. p. 37

FRIER, Sarah. **Zuckerberg Says Facebook Collects Internet Data on Non-Users.** Disponível em: <https://www.bloomberg.com/news/articles/2018-04-11/zuckerberg-says-facebook-collects-internet-data-on-non-users>. Acesso em: 01 jul. 2018.

GELLERT, Raphaël. Understanding data protection as risk regulation. **Journal of Internet Law**, vol., 18, n. 11, maio/2015. pp. 3-15.

GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado**. 1. ed. São Paulo: Atlas, 2017.

GORTÁZAR, Naiara Galarraga. **Facebook foi crucial para limpeza étnica do século XXI em Myanmar**. Disponível em: <https://brasil.elpais.com/brasil/2018/04/12/internacional/1523553344_423934.html>. Acesso em: 02 jul. 2018.

GRASSEGGER, Hannes; KROGERUS, Mikael. **How Cambridge Analytica used your Facebook data to help the Donald Trump campaign in the 2016 election**. Disponível em: <https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win>. Acesso em: 09 abr. 2018.

GRAU, Eros Roberto. **A ordem econômica na constituição de 1988**. São Paulo: Malheiros, 2006.

GUTWIRTH, Serge; HILDEBRANDT, Mireille. Some Caveats on Profiling. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul (ed.). **Data Protection in a Profiled World**. Dordrecht: Springer, 2010.

_____; LEENES, Ronald; DE HERT, Paul (ed.). **Data Protection on the Move**: Current Developments in ICT and Privacy/Data Protection. Law, Governance and Technology Series, Issues in Privacy and Data Protection, vol. 24. Dordrecht: Springer, 2015.

_____, et al (eds.). **Reloading Data Protection**: Multidisciplinary Insights and Contemporary Challenges. Dordrecht (Holanda): Springer, 2014.

GÜRSES, Seda; BERENDT, Bettina. **PETs in the Surveillance Society**: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul (ed.). **Data Protection in a Profiled World**. Dordrecht: Springer, 2010.

HARARI, Yuval Noah. **Homo Deus**: uma breve história do amanhã. Trad. Paulo Geiger. São Paulo: Cia. Das Letras, 2015. Edição em versão eletrônica (epub). Não paginado.

HAN, Byung-Chul. **La sociedad de la transparencia**. Trad. Raúl Gabás. Barcelona: Herder, 2013.

HASELTON, Todd. **Facebook explains how it can collect info about you even if you never post on Facebook**. Disponível em: <https://www.cnbc.com/2018/04/16/facebook-collects-data-even-when-youre-not-on-facebook.html>. Acesso em 01 jul 2018.

HERNKENHOFF, João Batista. **Como aplicar o Direito**: (à luz de uma perspectiva axiológica, fenomenológica e sociológico-política). Rio de Janeiro: Forense, 2010.

HILL, Kashmir. **How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did**. Disponível em: <http://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2>. Acesso em: 01 jul. 2018.

_____. **Facebook recommended a psychiatrist's patients friend each other — and there's no clear explanation**. Disponível em: <http://www.businessinsider.com/facebook-people-you-may-know-2016-8>. Acesso em: 14 set. 2017.

HERN, Alex; WATERSON, Jim. **Sites block users, shut down activities and flood inboxes as GDPR rules loom**. Disponível em: <https://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect>. Acesso em: 07 jun. 2018.

JACOBSON, Ralph. **2.5 quintillion bytes of data created every day**. How does CPG & Retail manage it? Disponível em: <https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it/>. Acesso em 13 jul. 2018.

JENTZSCH, Nicola. Monetarisierung der Privatsphäre: Welchen Preis haben persönliche Daten? **Deutsches Institut für Wirtschaftsforschung Wochenbericht**, n. 34, ago./2014, pp. 793-798. Disponível em: <https://www.diw.de/documents/publikationen/73/diw_01.c.479821.de/14-34-3.pdf>. Acesso em: 20 jun. 2018.

JORDÃO, Eduardo. RIBEIRO, Maurício Portugal. Como desestruturar uma agência reguladora em passos simples. **Revista Estudos Institucionais**, Vol. 3, n. 1, 2017, pp. 182-205.

KLEE, Antonia Espíndola Longoni. A regulamentação do uso da internet no Brasil pela Lei nº 12.965/2014 e a proteção dos dados e dos registros pessoais. **Direito & Justiça**, Porto Alegre, v. 41, n. 2, p. 126-153, jul.-dez. 2015.

KOTTASOVÁ, Ivana. **These companies are getting killed by GDPR**. Disponível em: <http://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html>. Acesso em: 07 jun. 2018.

KURBALIJA, Jovan. **Uma introdução à governança da internet**. Trad.: Carolina Carvalho. São Paulo: Comitê Gestor da Internet no Brasil, 2016.

LEENES, Ronald, et. al. (ed.). **Data Protection and Privacy**: (In)visibilities and Infrastructures. Dordrecht: Springer, 2017.

LEMOS, Ronaldo. **Lei de dados nasceu desgovernada.** Disponível em: <https://www1.folha.uol.com.br/colunas/ronaldolemos/2018/08/lei-de-dados-nasceu-desgovernada.shtml>. Acesso em: 22 ago. 2018.

LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2011.

LÉVY, Pierre. **Cibercultura**. Trad. Carlos Irineu da Costa. São Paulo: 34, 1999.

LEVIN, Sam. **Face-reading AI will be able to detect your politics and IQ, professor says**. Disponível em: <https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski>. Acesso em: 02 jul. 2018.

_____. **New AI can guess whether you're gay or straight from a photograph**. Disponível em: <https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph>. Acesso em: 14 set. 2017.

LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014.

LIMA, Caio César Carvalho. Garantia da privacidade e dados pessoais à luz do marco civil da internet. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014.

LIMA, Mariana. **Lei de Proteção de Dados brasileira é criada sem agência reguladora**. Disponível em: <https://link.estadao.com.br/noticias/cultura-digital,temer-sanciona-lei-de-protecao-de-dados-mas-veta-autoridade-regulatoria,70002451106>. Acesso em: 22 ago. 2018.

LUCHETE, Felipe. **Brasil é segundo país que mais manda Google apagar conteúdo da internet**. Disponível em; <http://www.conjur.com.br/2017-set-09/brasil-pais-manda-google-tirar-conteudo-internet>. Acesso em: 10 set. 2017.

LYON, David. **Theorizing Surveillance**: The panopticon and beyond. Cullompton: Willan, 2006.

MACAFEE, Andrew; BRYNJOLFSSON, Erik. **Big Data**: The Management Revolution. Harvard Business Review 90 (10), p.60-68. October 2012. Disponível em: <http://goo.gl/SmDmfp>. Acesso em: 15 nov. 2017.

MACHADO, Jorge; MORETTO, Márcio. Riscos e incertezas no uso do Facebook como plataforma de ativismo político. In: THEMOTEO, Reinaldo J. (Org.). **Cadernos Adenauer XVI, nº 3**: Internet e sociedade. Rio de Janeiro: Fundação Konrad Adenauer, 2015. pp. 113-132

MAIA, Vinícius Fernandes Costa; XAVIER, Yanko Marcius Alencar. Relação da qualidade do Diesel brasileiro, a redução do teor de enxofre promovida pelo PROCONVE. In: XAVIER, et. al (org.). **Proteção do meio ambiente na indústria do petróleo e gás natural**. Natal: EDUFRN, 2016. p. 299-316.

MANOLESCU, Dan. **Data protection as a fundamental right**. Effectius, Brussels, n. 5, jun./2010. Disponível em: <http://effectius.com/yahoo_site_admin/assets/docs/Data_protection_as_a_fundamental_right_Dan_Manolescu_Issue5.16761659.pdf>. Acesso em 15 jul. 2018.

MARCACINI, Augusto Tavares Rosa. **Direito e Informática**: uma abordagem jurídica sobre a criptografia. Rio de Janeiro: Forense, 2002.

MARCHETTI, Brunno. **Alckmin acionou Justiça para descobrir IP de quem o xingou muito no twitter**. Disponível em: <https://motherboard.vice.com/pt_br/article/78wzv9/alckmin-acionou-justica-para-descobrir-ip-de-quem-o-xingou-muito-no-twitter>. Acesso em 08 jul. 2018.

MARQUES NETO, Floriano de Azevedo; FREITAS, Rafael Véras de. Uber, WhatsApp, Netflix: os novos quadrantes da publicatio e da assimetria regulatória. **Revista de Direito Público da Economia – RDPE**, Belo Horizonte, ano 14, n. 56, p. 75-108, out./dez. 2016.

MATHEWS, Lee. **Equifax Data Breach Impacts 143 Million Americans**. Disponível em: <https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#248efd3f356f>. Acesso em: 15 set. 2017.

MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. Dissertação (Mestrado em Direito). Brasília: Universidade de Brasília, 2008.

MENEZES NETO, Elias Jacob de. **Surveillance, democracia e direitos humanos**: os limites do Estado na era do big data. Tese (Doutorado em Direito). São Leopoldo: UNISINOS, 2016.

MOLON, Alessandro. A legislação e a internet. In: THEMOTEO, Reinaldo J. (Org.). **Cadernos Adenauer XVI, nº 3**: Internet e sociedade. Rio de Janeiro: Fundação Konrad Adenauer, 2015. pp. 97-112.

MONTEIRO, Renato Leite. **Presidente Temer, a lei de dados precisa de seu órgão fiscalizador**. Disponível em: <https://brasil.elpais.com/brasil/2018/07/13/opinion/1531506142_357368.html>. Acesso em: 24 jul. 2018.

MOREIRA, Egon Bockmann. Agências reguladoras independentes, poder econômico e sanções administrativas. In: PECI, Alketa (org.). **Regulação no Brasil:** desenho, governança, avaliação. São Paulo: Atlas, 2007.

MURRAY, Andrew. **Information technology law**: the law and society. New York: Oxford University Press, 2010.

NARAYANAN, Arvind; HUEY, Joanna; FELTEN, Edward J. A Precautionary Approach to Big Data Privacy. pp. 357-386 In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (ed.). **Data Protection on the Move**: Current Developments in ICT and Privacy/Data Protection. Law, Governance and Technology Series, Issues in Privacy and Data Protection, vol. 24. Dordrecht: Springer, 2015.

NISSENBAUM, Helen. **Privacy in context:** technology, policy and the integrity of social life. Stanford: Stanford University, 2010.

ORRÙ, Elisa. Minimum Harm by Design: Reworking Privacy by Design to Mitigate the Risks of Surveillance. In: LEENES, Ronald, et. al. (ed.). **Data Protection and Privacy**: (In)visibilities and Infrastructures. Dordrecht: Springer, 2017. pp. 107-138.

PASSOS, Bruno Ricardo dos Santos. **O direito à privacidade e a proteção aos dados pessoais na sociedade da informação**: uma abordagem acerca de um novo direito fundamental. Dissertação (Mestrado – Direito). Salvador: UFBA, 2017. 102 f.

PÁDUA, Luciano. **‘Precisamos de uma geração de engenheiros legais’, diz Richard Susskind**.

Disponível em: <https://www.jota.info/carreira/susskind-futuro-direito-05062018>. Acesso em 25 jun. 2018.

PECI, Alketa. Regulação comparativa: uma (des)construção dos modelos regulatórios. In:_____. (org.). **Regulação no Brasil:** desenho, governança, avaliação. São Paulo: Atlas, 2007.

PINHO, José Antonio Gomes de. **Sociedade da informação, capitalismo e sociedade civil:** reflexões sobre política, internet e democracia na realidade brasileira. RAE, São Paulo, v. 51, n. 1, jan./fev. 2011, pp. 98-106.

PRINCETON. **The world's most valuable resource is no longer oil, but data**. Disponível em: <https://www.economist.com/lealdades/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em 15 set. 2017.;

RAMOS, Pedro Henrique Soares. Neutralidade da rede e Marco Civil da Internet: um guia para interpretação. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014. pp. 165-187.

REINALDO FILHO, Demócrito R. **Privacidade na Sociedade da Informação**. Dissertação (Mestrado em Direito). Recife: Universidade Federal de Pernambuco. 2006.

RONCOLATO, Murilo. **O que diz o projeto de lei de proteção de dados que tramita no Senado**. Disponível em: <https://www.nexojornal.com.br/expresso/2018/06/07/O-que-diz-o-projeto-de-lei-de-prote%C3%A7%C3%A3o-de-dados-que-tramita-no-Senado>. Acesso em: 08 jul. 2018.

RODOTÀ, Stefano. **El derecho a tener derechos**. Tradução de José Manuel Revuelta Lopez. 1. ed. Madrid: Trotta, 2014.

ROTELLA, Perry. **Is Data The New Oil?** Disponível em: <https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#62c474087db3>. Acesso em: 15 set. 2017.

RUARO, Regina Linden. **A tensão entre o direito fundamental à proteção de dados pessoais e o livre mercado**. REPATS, Brasília, v. 4, n. 1, p. 389-423, Jan-Jun, 2017.

_____; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. **Revista da Faculdade de Direito** - UFPR, Curitiba, n. 47, p.29-64, 2011.

_____. Privacidade e Autodeterminação Informativa: obstáculos ao Estado de Vigilância? **Arquivo Jurídico,** Teresina/PI, v. 2, n. 1, jan./jun. de 2015, p. 41-60.

SANDERS, James. **To save thousands on GDPR compliance, some companies are blocking all EU users**. Disponível em: <https://www.techrepublic.com/article/to-save-thousands-on-gdpr-compliance-some-companies-are-blocking-all-eu-users/>. Acesso em: 07 jun. 2018.

SARDETO, Patricia Eliane da Rosa. **Tratamento informatizado de dados pessoais e o direito à privacidade**. Dissertação (Mestrado em Direito), Florianópolis: Universidade Federal de Santa Catarina, 2004.

SARMENTO, Daniel. **Direitos Fundamentais e Relações Privadas**. 2ª ed. Rio de Janeiro: Lumen Juris, 2010.

SILVA, Alexandre Pacheco da (Coord.). **Um novo mundo de dados**: relatório final. São Paulo: FGV, 2017.

SILVA, Marcos Sergio. **Juiz dribla Marco Civil e dá a Doria direito de identificar críticos no Facebook**. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2017/04/21/juiz-dribla-marco-civil-e-da-a-doria-direito-de-identificar-criticos-no-facebook.htm>. Acesso em 08 jul. 2018.

SOLOVE, Daniel J. **Nothing to hide**: the false tradeoff between privacy and security. London: Yale University, 2011.

_____. **The Digital Person**: technology and privacy in the information age. New York: New York University Press, 2004.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco Civil da Internet**: construção e aplicação. Juiz de Fora: Editar, 2016.

SPARROW, Andrew. **The law of virtual worlds and Internet social networks**. Gower: Farnham, 2012.

STEIJN, Wouter Martinus Petrus. The Cost of Using Facebook: Assigning Value to Privacy Protection on Social Network Sites Against Data Mining, Identity Theft, and Social Conflict. In: GUTWIRTH, Serge, et al (eds.). **Reloading Data Protection**: Multidisciplinary Insights and Contemporary Challenges. Dordrecht (Holanda): Springer, 2014. pp. 323-342

SUMNER, Stuart. **You: for sale** – protecting your personal data and privacy online. Waltham: Elsevier, 2016.

SUPPO, Hugo Rogelio. Internet e democracia. In: THEMOTEO, Reinaldo J. (Org.). **Cadernos Adenauer XVI, nº 3**: Internet e sociedade. Rio de Janeiro: Fundação Konrad Adenauer, 2015. pp. 19-45.

TANNER, Adam. **What stays in Vegas**: the world of personal data — lifeblood of big business — and the end of privacy as we know it. New York: PublicAffairs, 2014.

TAVARES, André Ramos. **Direito Constitucional Econômico**. 3 ed. São Paulo: Método, 2011.

TECHDIRT. **Companies Respond To The GDPR By Blocking All EU Users**. Disponível em: <https://abovethelaw.com/2018/05/companies-respond-to-the-gdpr-by-blocking-all-eu-users/>. Acesso em: 07 jun. 2018.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar**, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017.

THEMOTEO, Reinaldo J. Cibercultura e participação política no Brasil. In: _____ (Org.). **Cadernos Adenauer XVI, nº 3**: Internet e sociedade. Rio de Janeiro: Fundação Konrad Adenauer, 2015. pp. 7-17. p. 13

_____; (Org.). **Cadernos Adenauer XVI, nº 3**: Internet e sociedade. Rio de Janeiro: Fundação Konrad Adenauer, 2015.

THE MATRIX (**Matrix**), Direção e roteiro: Andy Wachowski e Larry Wachowski, Produção Joel Silver. Distribuição: Warner Bros. EUA, 1999.

VAINFAS, Ronaldo. **História da vida privada**: dilemas, paradigmas, escalas. Anais do Museu Paulista. São Paulo. n. sér. v. 4 p. 9-27 jan./dez. 1996.

VANIAN, Jonathan. **Why Data Is The New Oil**. Disponível em: <http://fortune.com/2016/07/11/data-oil-brainstorm-tech/>. Acesso em: 15 set. 2017.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Dissertação (Mestrado em Direito). Brasília: UnB, 2007.

VILLAS BOAS FILHO, Orlando. A governança em suas múltiplas formas de expressão: o delineamento conceitual de um fenômeno complexo. **Revista Estudos Institucionais**, vol. 2, n. 2, 2016, pp. 673-698.

WAGNER, Kurt. **Facebook's 'People You May Know' feature can be really creepy. How does it work?** Disponível em: <https://www.recode.net/2016/10/1/13079770/how-facebook-people-you-may-know-algorithm-works>. Acesso em: 01 jul. 2018**.**

WALL, Mathew. **Big data**: are you ready for blast-off? Disponível em: <https://www.bbc.co.uk/news/business-26383058>. Acesso em 13 jul. 2018.

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. **Harvard Law Review**, v. IV, dez. 1890, n. 5. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 10 jan. 2017.

WHATSAPP. **Criptografia de ponta-a-ponta**. Disponível em: <https://faq.whatsapp.com/pt_br/android/28030015/>. Acesso em: 07 jul. 2018.

WU, Tim. **Impérios da comunicação**: do telefone à internet, da AT&T ao Google. Trad. Cláudio Carina. Zahar: Rio de Janeiro, 2012. Não paginado (epub).

_____. **The Attention Merchants**: the epic scramble to get inside our heads. New York: Alfred A. Knopf, 2016. Não paginado (epub).

ZARSKY, Tal. Responding to the Inevitable Outcomes of Profiling: Recent Lessons from Consumer Financial Markets, and Beyond. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul (ed.). **Data Protection in a Profiled World**. Dordrecht: Springer, 2010.

ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do right of privacy nos estados unidos. **Revista Brasileira de Direito Civil** | ISSN 2358-6974 | Volume 3 – Jan / Mar 2015. pp. 8-27. Disponível em: <https://www.ibdcivil.org.br/image/data/revista/volume3/02---rbdcivil-volume-3---o-surgimento-e-o-desenvolvimento-do-right-of-privacy-nos-estados-unidos.pdf>. Acesso em: 07 maio 2018. p. 11

ZANATTA, Rafael. **Proteção de dados pessoais como regulação do risco:** uma nova moldura teórica? In: I ENCONTRO DA REDE DE GOVERNANÇA DA INTERNET, 2017, Rio de Janeiro. 20 pp.

_____. A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet, in: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. **Direito e Internet III**: Marco Civil da Internet. São Paulo: Quartier Latin, 2015. p. 447-470.

ZANFIR, Gabriela. Forgetting About Consent. Why The Focus Should Be On “Suitable Safeguards” in Data Protection Law. In: GUTWIRTH, Serge, et al (eds.). **Reloading Data Protection**: Multidisciplinary Insights and Contemporary Challenges. Dordrecht (Holanda): Springer, 2014. pp. 237-258.

GLOSSÁRIO

Big data	Termo surgido para designar, inicialmente, enormes quantidades e volume de dados oriundos da Astrofísica, mas que, atualmente, se utiliza para designar um cenário relacionado às TIC, de vasta quantidade de dados, de diferentes origens e tipos, e as ferramentas e soluções adequadas para o seu aproveitamento.
Code is law	Em poucas palavras, "código (informático) é Lei". Expressão criada por Lawrence Lessig para dizer que os códigos, por terem a capacidade de construir e padronizar uma realidade, possuem força semelhante às leis.
Cookies	Pequenos arquivos de computador lançados por *websites* nos dispositivos (computadores, *smartfones*, etc) que os acessam, de forma que estes dispositivos possam ser identificados pelo servidor do *website* do qual o *cookie* se originou. São lançados, muitas vezes, compulsoriamente, sem que o usuário tenha escolha (ou mesmo ciência) acerca de sua utilização. Muito utilizado para oferecer experiências personalizadas aos usuários.
Dataísmo	Termo utilizado pelo historiador e filósofo israelense Yuval Noah Harari para designar uma abordagem científica acerca da realidade que crê na primazia dos dados. Para esta abordagem, toda e qualquer expressão empírica da vida pode ser reduzida em forma de dados, desde a biologia, passando pela economia, relações sociais, comportamento, até chegar às tecnologias de diferentes matizes. Partindo deste pressuposto, preconiza que qualquer situação é passível de análise atuarial, estatística e probabilística, de forma que, eventualmente, ferramentas como algoritmos e inteligências artificiais possam lidar com o tratamento destes dados com a maior eficiência possível, suplantando a necessidade da presença humana.
Dataveillance	Expressão criada para denotar a prática da *surveillance* através da coleta e tratamento de dados pessoais, fazendo a junção das palavras *data* (dados, em inglês) e *surveillance* (vigilância).
Privacy by design	Conjunto de práticas que procuram incutir, em procedimentos e estruturas inerentes a uma prática ou serviço, medidas que protejam a privacidade dos usuários.
Surveillance	Prática de vigilância de cidadãos ou grupos e coletividades que pode ser oriunda tanto do Estado como de entes privados, com as mais diversas

finalidades (antiterrorismo, segurança nacional, perseguição política, religiosa, etc) e por meio de diferentes técnicas.